CNS - COMPUTER NETWORK SECURITY (CNS)

CNS 2003 Enterprise Network Services (2-2-3)
Explore concepts and technologies behind domain based enterprise networks. Install, configure and administer an enterprise network operating system and configure protocols, services and server functions such as storage, backup and disaster recovery to the level required to effectively administer a secured domain based enterprise networks.
Prerequisites: CIS 1103

CNS 2103 Network Fundamentals (2-2-3)
Exploring the OSI and TCP/IP layered models is fundamental to understanding how computing devices communicate with each other. Analyse the role the various protocols play in relation to physical and logical addressing, network types, end-to-end connectivity and application requirements and develop abilities to assess key factors in designing and building effective computer networks.
Prerequisites: CIS 1103

CNS 3003 Switching and Routing Essentials (2-2-3)
Discuss the features of layer 2 and layer 3 switchings, and learn how a switch interconnects and communicates with other switches and routers. Understand how routers learn about remote networks and configure static or default routing on the routers to direct data packets to reach a final destination. Build efficient, secure, and reliable switched networks of varying sizes in response to business needs and apply effective troubleshooting techniques to ensure reliable communication between all devices on the network.
Prerequisites: CNS 2103 or CIS 2103

CNS 3023 Network Security and Cryptography (2-2-3)
Investigate the principles of network security, including identifying system attacks and countermeasures. Discuss the basic concepts of cryptography using various encryption standards and techniques. Analyze public-key infrastructure, digital signatures, and hash functions. Configure network devices, including routers and firewalls, to prevent network attacks and protect vital business assets. Apply network security and encryption technologies to secure various computing domains.
Prerequisites: (CNS 2103, CIS 2103) or (CIN 2103, CIS 2103)

CNS 3113 Cyber Law and Ethics (3-1-3)
The course provides an insight into the laws and regulations of cyberspace, from a general understanding of the legal issues in information systems security and privacy, to the legal, managerial, and ethical issues affecting technology-enabled organizations.
Prerequisites: CIS 2103

CNS 3123 Intrusion Detection and Ethical Hacking (2-2-3)
The course utilizes intrusion detection techniques for the purpose defending and securing organizational information infrastructures. The students will be identifying methods used in computer and network hacking in order to better protect systems from such intrusions. Describing the role of a penetration tester, including what an ethical hacker do legally. Examining different types of malicious software. Implementing hacking and tools and techniques to determine potential system vulnerabilities. Reflecting on the purpose of defending organizational and information infrastructure.
Prerequisites: CIS 2903

CNS 3203 Enterprise Networking, Security and Automation (2-2-3)
Select and configure dynamic routing protocols and implement enterprise solutions such as Access Control Lists (ACLs) and Network Address Translation (NAT) to create secure network connectivity within organizations and to the Internet. Discuss Wide Area Network (WAN) architectures and broadband access technologies used in the design of secured enterprise and broadband networks. Implement various WAN connectivity options used to satisfy business requirements. Provide the skills and knowledge to design, build and troubleshoot enterprise network solutions in response to complex business scenarios
Prerequisites: CNS 3003 or CIN 3003