CSF - SECURITY AND FORENSICS (CSF)

CSF 2113 Programming for Information Security (2-2-3)
The course develops the necessary coding skills for the Security and Forensics students to carry out security related tasks. Students will be Identifying building blocks of a specific scripting language to develop scripts that fulfill the requirements for automating tasks, finding weaknesses, exploiting vulnerabilities, and many other security and forensics related objectives.
Prerequisites: CIS 2903, ICT 2013

CSF 3003 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 e-commerce security and privacy, to the legal, managerial, and ethical issues affecting technology enabled organizations.
Prerequisites: CIS 2103

CSF 3103 Incidence Response and Disaster Recovery (3-1-3)
The course develops two threads: Analyzing and responding to attacks, and recovering the system from attacks or disasters. The student will be prioritizing attacks facing an organization using a weighted analysis table. Recovering from attacks, incidents and disasters by implementing a variety of tools. Identifying system vulnerabilities, taking appropriate countermeasures, developing an incident response and recovery plan and finally implementing a disaster recovery plan to minimize downtime.
Prerequisites: CIN 2103

CSF 3203 Intrusion Detection and Ethical Hacking (2-2-3)
The course utilises intrusion detection techniques for the purpose defending and securing organisational 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 organisational and information infra-structure.
Prerequisites: CIS 2903

CSF 3403 Computer Forensics and Investigation (2-2-3)
The course analyses various computer systems that have been compromised. The student will be performing a systematic investigation, recovering critical data and aiding authorities in tracking those who caused the security breach. Analysing and investigating digital evidence as related to UAE Cyber Law. Producing evidence for presentation in a UAE court of law. Analysing crime incident reports using software and hardware computer forensics tools. Recovering digital data using forensics techniques. Developing a report of the breach.
Prerequisites: CIN 2003

CSF 3603 Cryptography and Network Security (2-2-3)
The course introduces key concepts of encryption such as ciphers, symmetric and asymmetric encryption. The student will be identifying system attacks and countermeasures. Recognising the basic concepts of cryptography using various encryption techniques. Analysing public key infrastructure, digital signatures and hash functions. Applying cryptosystems to user authentication, email, IP/web security and wired and wireless networks.
Prerequisites: CIS 2103

CSF 4003 Security and Risk Management (2-2-3)
This course recognizes information security from the perspective of risk management. The course discusses key information security management concepts and organizational roles for access, control, and business continuity management. Students will learn methods of information security risk assessment, intellectual property protection, organizational structure assessment, threat modeling for critical infrastructure protection, manage the risk via contingency planning to reduce unexpected events, implementing analytical tools for quantifying risk, and the costs and benefits of mitigation tools.
Prerequisites: CSF 3403 or CIS 2103

CSF 4103 Web Application and E-Commerce Security (2-2-3)
The course discovers and exploits security flaws and major vulnerabilities inherent in web applications. The student will be applying various tools for mapping an e-commerce web application in order to identify its vulnerabilities. Identifying tools and techniques to secure vulnerabilities in client-side controls, authentication, session management, and access controls. Initiating injection attacks, and appropriate countermeasures to test and secure web applications such as online banking and e-commerce. Applying various defense mechanisms to secure web applications against possible attacks.
Prerequisites: CSF 3603, CSF 3203

CSF 4203 Telecommunications and WAN Security (2-2-3)
The course Identifies different data communication and transmission techniques in telecommunication and WAN. The student will be discussing TCP/IP and OSI protocol reference models and configuring circuit-switching and packet-switching technologies. Implementing various WAN protocols including Frame relay, ATM, MPLS and Wireless WAN. Designing and configuring WAN technologies and VPN for business data communications.
Prerequisites: CSF 3603

CSF 4613 Security Intelligence (2-2-3)
The course expresses a more developed understanding of the anomalies and suspicious activities related to Information Technology. The student will be exploring a deep visibility into network, user, application activity, and Security Information and Event Management. Consolidating security's relevant data from various sources to perform in-depth analysis, and to investigate threats and generate reports that meet compliance and standard regulatory schemes.
Prerequisites: CIS 2103