CYBER SECURITY (CSEC)

CSEC 5300 Research Seminar
Credits: 3 (3-0-0)
This course is focused on developing a student's research skills. Students will be guided through research of peer-reviewed journal articles and research methodologies as they relate to the field of cyber security. The instructor will guide students through a written review of research methodologies and current practices.

Restrictions:

CSEC 5304 Database Security
Credits: 3 (3-0-0)
This course focuses on the protection of data at rest. The course covers subjects in databases and DBMS related to security. Examples of subjects include: DB access control and identity management, DB architecture, password policies, DB auditing, privileges, and roles administration.

Restrictions:

CSEC 5306 Computer Networks and Security
Credits: 3 (3-0-0)
This course will cover advanced topics in computer networks, such as, wireless networks, cloud and Big Data networks. Students will gather knowledge on the vulnerabilities in different types of networks, detection methods, and "state-of-the-art" techniques to prevent them. Other subjects include: Wireless, mobile and cloud network vulnerabilities and detection methods, defense techniques, moving target techniques and network access controls.

Restrictions:

CSEC 5310 Advanced Topics in Computer Forensics
Credits: 3 (3-0-0)
This course is an overview of the methods and tools utilized for collecting and preserving electronic digital evidence for the computer forensic process. Topics include the forensic examination, analysis, and report writing; and preparing for courtroom testimony about the forensic results.

Restrictions:

CSEC 5311 Big Data Analysis and Security
Credits: 3 (3-0-0)
This course will introduce students to the concepts, principles, and application of big data and big data analytics and security. It will provide knowledge and practical experience on big data analytics tools and platforms including MapReduce, Hadoop, and Spark which leverage big data to solve current business problems. Moreover, this course will cover recent advanced techniques to secure big data while it is in rest (storage) and/or in motion (over networks).

Restrictions:

CSEC 5321 Information Assurance and Risk Management
Credits: 3 (3-0-0)
This course concentrates on security governance structure that organizations employ to manage risks. Various laws, regulations, and organizational objectives are typically mapped to organizational policies and translated into procedures, practices, standards, and guidelines. Topics covered include social engineering, risk assessment, recovery and response, enterprise security, and formal techniques and policies.

Restrictions:

CSEC 5322 Identity Management and Access Control
Credits: 3 (3-0-0)
This course covers subjects related to using access control techniques and mechanisms to appropriately address security requirements such as (CIAAA): confidentiality, integrity, authentication, authorization, and accountability. Main topics include access control principles, mechanisms, and techniques (e.g., ABAC, OBAC, RBAC) related to user identification and strategies for enabling stronger authentication, using Public-Key Infrastructure (PKI), and other enterprise identity management technologies, industry standards for enabling identity provisioning, single sign-on, and identity federation

Restrictions:

CSEC 5323 Cryptography and Secure Communication
Credits: 3 (3-0-0)
This course introduces the basic concepts of cryptography. Various cipher systems are presented including symmetric versus asymmetric encryption systems. The course focuses also on applications of cryptography in the different domains. Methods used to attack ciphers are also discussed. Different case studies of use of cryptographic methods in the different domains are presented as part of students labs and projects.

Restrictions:

CSEC 5326 Security in Emerging Technologies
Credits: 3 (3-0-0)
This course will cover security aspects in one or more of state-of-the-art emerging technologies such as mobile computing, world wide web, online social networks, cloud computing, IoT, cyber physical systems, etc. Instructor can pick one or more of those technologies based on their research interests.

Restrictions:

CSEC 5327 Advanced Information Security
Credits: 3 (3-0-0)
This course examines the concepts, principles, and applications of computer security in the business environment including Privacy, Information Security, and Critical Infrastructure. This course explores the knowledge and skills needed to ensure security of information and information systems within organizations. It focuses on concepts and methods associated with security across several systems platforms, including internal and Internet-based systems. The course utilizes a world view to examine critical infrastructure concepts as well as techniques for assessing risk associated with accidental and intentional breaches of security in a global network. It introduces the associated issues of ethical uses of information and of privacy considerations.

Restrictions:

CSEC 5333 Programming for Cyber Security
Credits: 3 (3-0-0)
This course will Introduce Python programming language for information and cyber security applications. Students will learn the necessary theoretical background in the lecture and will learn writing Python codes in the lab for different subjects including: socket communication, web security and testing, penetration testing, ethical hacking tools and applications, encryption, operating system communication and APIs, etc.

Restrictions:

CSEC 5350 Intrusion Detection and Hackers Exploits
Credits: 3 (3-0-0)
This course explores the growing challenges of securing sensitive data networks, mobile devices and applications with different privacy controls to defend against malicious acts. Also, this course addresses new trends in computer science and how machine learning and anti-malware defenses can respond to threats, and protect networks, infrastructure and users.

Restrictions:

CSEC 5370 Special Topics in Cyber Security
Credits: 3 (3-0-0)
Special topics related to cyber security determined by the instructor based on their research interests.

Restrictions:

CSEC 5380 Cyber incident response
Credits: 3 (3-0-0)
This course will cover different subjects related to the lifecycle of incident management including incident detection, reporting and handling. The course includes technical and non technical subjects. Examples of non-technical subjects: business impact analysis (BIA), a business continuity plan (BCP) and a disaster recovery plan (DRP). Examples of technical subjects: Tools related to incident detection and vulnerability assessment, attack types analysis, methods to analyze artifacts left on compromised systems, and different types of Indicators of Compromise (IoC).

Restrictions: