Year 1

CSEC 1310 - Intro to Cyber Security

3 credit hours.

Introduction to the cybersecurity discipline and the crosscutting concepts related to cybersecurity thought.

Year 2

CSEC 2310 - System Security

3 credit hours.

Covers the holistic concept of a cyber system of people, processes, technology and data organized as a unit, understanding how to develop security requirements and selection of controls to meet requirements. This course also addresses the security issues of connecting components and using them within larger systems.

CSEC 2320 - Access Control

3 credit hours.

Covers logical and physical access control policy and mechanisms for cyber systems. Also covers the role of authorization, identification, authentication and monitoring in access control.

CSEC 2324 - Network Security

3 credit hours.

Fundamentals in network protocols and design, routing, local and wide area communications and wireless networks. This course will also cover inherent security design flaws and network attack as well as network defense mechanisms, including firewalls, intrusion detection systems and an introduction to secure protocols.

Year 3

CSEC 3312 - Applied Cryptography

3 credit hours.

A survey and study of the major cryptographic techniques, algorithms, and implementations, with emphasis on applications to data security and network security. Intended as a practical

CSEC 3314 - Incident Response

3 credit hours.

Cybersecurity incidents are inevitable for organizations. This course prepares students for the lifecycle of planning for, responding to and recovering from cybersecurity incidents.

introduction to the current state-of-the-art of cryptographic usage.	Topics include (i) the technical mechanisms for log review, identification, containment and eradication and (ii) the organizational management of cybersecurity incident response, business continuity and disaster recovery functions.
CSEC 3316 - Threat Analytics (Elective) 3 credit hours. Understanding the adversarial threat and mechanisms to identify and mitigate threats in real time. This course covers (i) the various types of adversaries to consider when protecting cyber systems, (ii) threat hunting using system generated audit logs and network traffic, and (iii) threat intelligence gathering and sharing.	**CSEC 3320 - IoT Security (Elective)** 3 credit hours. Covers the Internet of Things (IoT) and fog computing model, cybersecurity challenges with IoT, mechanisms for high assurance and automated maintenance in secure operations. This course explores various threat models and societal impacts associated with broad IoT cyber attacks.
CSEC 3322 - Software Security 3 credit hours. Covers fundamental design principles and security requirements for secure software development, mitigating common software security flaws, and testing for software security vulnerabilities.	**CSEC 3324 - Data Security** 3 credit hours. Covers the security of data at rest, during processing, and in transit. Specific topics include database security, file encryption, data integrity, authentication, destruction and data security law.
CSEC 3300 - Digital Forensics 3 credit hours. Covers the legal, technical and procedural methodologies associated with digital forensic investigations.	
Year 4	
CSEC 4310 - Risk Management 3 credit hours. Covers the practices necessary for organizations to manage cybersecurity risk in support of the organization’s mission. This course includes topics on cybersecurity (i) risk	**CSEC 4312 - Cloud Security (Elective)** 3 credit hours. Covers virtualization and cloud infrastructure and the assurance necessary to provide secure cloud architectures. Specific topics include network security, cryptographic key

assessment, (ii) governance and policy and (iii) strategy and planning.	management, data security and threat hunting in relation to the cloud computing environment.
CSEC 4314 - Human Behavior and Privacy 3 credit hours. Covers human interaction in the security of cyber systems, including adversarial threats, understanding the way humans interact with cybersecurity controls and the personal impacts cybersecurity has on humans.	**CSEC 4318 - Vulnerability Management (Elective)** 3 credit hours. Covers software flaw remediation, exploit development, penetration testing and the continuous organizational processes for managing the risk introduced by software vulnerabilities. This course also covers the data models and automation procedures for managing vulnerabilities.
CSEC 4320 - Cybersecurity Legal and Compliance 3 credit hours. Covers ethics, laws and policies related to cybersecurity. This course familiarizes students with the practice of law in relation to cybercrime and covers various regulatory and standards frameworks. Students will understand the global, social, economic and legal impacts of cybersecurity in society.	**CSEC 4322 - Malware Analysis (Elective)** 3 credit hours. A thorough analysis of malware including cutting edge techniques to detect malware, protect against it and track malware through the phases of an attack. This course also covers the technical analysis and investigation of current malicious code for the purpose of developing better protection mechanisms.
CSEC 4395 - Cyber Security Capstone I **CSEC 4396 - Cyber Security Capstone II** 6 credit hours.	