# CYBER SECURITY (CSEC)

**CSEC 1360 Security Tools I**
**Credits:** 3 (3-0-0)
This course introduces cyber security tools and provides hands-on practice using these tools. Students learn Linux/Unix based security assessment tools and operating systems through hands-on security testing and experimentation. TSI Restriction(s): Math, Reading, Writing.

**Restrictions:** Graduate level students may not enroll.

**CSEC 1436 Cyber Security Prog I + Lab**
**Credits:** 4 (0-0-0)
Course covers introductory programming for cyber security applications such as forensics, penetration testing, cryptography, etc. Introductory python structures, features, and modules are used for developing these applications. Course includes lab component for lab-based exercises. TSI Restriction(s): Reading, Math, and Writing

**Prerequisites:** Grade of C or better in each: MATH 1314 or equivalent.

**Restrictions:** Graduate level students may not enroll.

**CSEC 1437 Cyber Security Prog II + Lab**
**Credits:** 4 (0-0-0)
Course covers intermediate level programming for cyber security applications such as forensics, penetration testing, cryptography, web programs, etc. Appropriate cyber security related python structures, features and modules are used for developing these applications. Course includes lab component for lab-based exercises. TSI Restriction(s): Reading, Math, and Writing

**Prerequisites:** Grade of C or better in each: MATH 1314 or equivalent, CSEC 1436.

**Restrictions:** Graduate level students may not enroll.

**CSEC 2306 Computer Networks**
**Credits:** 3 (3-0-0)
This course covers subjects related to computer networks including TCP/IP and OSI models, network applications, distributed systems and an introduction to network security. The course focuses on concepts, principles and technologies that enable the integration of information and telecommunications systems for support of internal and external business activities. TSI Restriction(s): Reading, Math, and Writing. Graduate level students may not enroll.

**Prerequisites:** Grade of 'C' or better in each: MATH 1314 or equivalent.

**Restrictions:** Graduate level students may not enroll.

**CSEC 2325 Hardware Security**
**Credits:** 3 (3-0-0)
This course focuses on hardware security and covers security and trust from the hardware perspective. This course introduces students to hardware components including System on Chip (SoC) and Printed Circuit Board (PCB) and examines security and trust issues in such hardware components. It also covers hardware security threats, malware, and attacks along with specific countermeasures against hardware attacks. TSI Restriction(s): Reading, Math, and Writing. Graduate level students may not enroll.

**Prerequisites:** Grade of 'C' or better in each: MATH 1314 or equivalent, CSEC 1436 or CSCI 1436 or (CSCI 1336 and CSCI 1136), CSEC 1437 or CSCI 1437 or (CSCI 1336 and CSCI 1137).

**Restrictions:** Graduate level students may not enroll.

**CSEC 2336 Cyber Security Applications**
**Credits:** 3 (3-0-0)
Course covers development of cyber security applications for forensics, penetration testing, cryptography, web programs, etc. Appropriate cyber security related python structures, features and modules are used for developing these applications. TSI Restriction(s): Reading, Math, and Writing

**Prerequisites:** Grade of C or better in each: MATH 1314 or equivalent, CSEC 1436, CSEC 1437.

**Restrictions:** Graduate level students may not enroll.

**CSEC 2341 Web App Progs for Security**
**Credits:** 3 (3-0-0)
This course introduces web scripting/programming, such as Java scripting, PHP, etc. for web services and applications security assessment. Students learn web scripting/programming with an emphasis on the skills of detecting and assessing potential security vulnerabilities in web services and applications.

**Prerequisites:** A grade of C or better in each of : Math 1314 or equivalent, CSEC 1436 or CSCI 1436 or (CSCI 1336 and CSCI 1136), CSEC 1437 or CSCI 1437 or (CSCI 1337 and CSCI 1137).

**Restrictions:** Graduate level students may not enroll.

**CSEC 2356 Systems Analysis and Design**
**Credits:** 3 (3-0-0)
Analysis and design techniques required for implementing medium to large-scale computer information systems. Development of requirements for personnel, software and equipment for typical applications. TSI Restriction(s): Reading, Math, and Writing. Graduate level students may not enroll.

**Prerequisites:** Grade of 'C' or better in each: MATH 1314 or equivalent, CSEC 1436 or CSCI 1436 or (CSCI 1336 and CSCI 1136).

**Restrictions:** Enrollment is limited to students with a major in Cybersecurity.Graduate level students may not enroll.

**CSEC 2360 Security Tools II**
**Credits:** 3 (3-0-0)
This course introduces students to common web application security testing tools and the Metasploit Framework. Students will practice using these tools to assess security vulnerabilities in Internet services and web applications. Ethical standards related to the use of security tools will be emphasized. TSI Restriction(s): Reading, Math, and Writing. Graduate level students may not enroll.

**Prerequisites:** Grade of 'C' or better in each: MATH 1314 or equivalent, CSEC 1360.

**Restrictions:** Graduate level students may not enroll.

**CSEC 3309 Scripting Languages**
**Credits:** 3 (3-0-0)
This course introduces students to common scripting languages used in computing. It examines the overall design of scripting languages as well as the specific syntax of common scripting languages. Students will develop projects in each of the languages examined and will determine the best application environment for each of the languages examined. TSI Restriction(s): Reading, Math, and Writing. Graduate level students may not enroll.

**Prerequisites:** Grade of 'C' or better in each: MATH 1314 or equivalent, CSEC 1436 or CSCI 1436 or (CSCI 1336 and CSCI 1136), CSEC 1437 or CSCI 1437 or (CSCI 1336 and CSCI 1137).

**Restrictions:** Graduate level students may not enroll.

**CSEC 3321 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 and explores the knowledge and skills needed to ensure security of information and information systems within organizations. TSI Restriction(s): Reading, Math, and Writing. Graduate level students may not enroll.

**Prerequisites:** Grade of 'C' or better in each: MATH 1314 or equivalent, CSEC 2306 or CISA 2306.

**Restrictions:** Enrollment is limited to students with a major in Cybersecurity.Graduate level students may not enroll.

**CSEC 3325 Network Security**
**Credits:** 3 (3-0-0)
The course explores mechanisms for protecting networks against attacks with an emphasis placed on network security applications for the Internet and corporate networks. The course also investigates various networking security standards and explores methods for enforcing and enhancing those standards. TSI Restriction(s): Reading, Math, and Writing. Graduate level students may not enroll.

**Prerequisites:** Grade of 'C' or better in each: MATH 1314 or equivalent, CSEC 1436 or CSCI 1436 or CSCI 1336 and CSCI 1136, CSEC 3321 or CISA 3321.

**Restrictions:** Enrollment is limited to students with a major in Cybersecurity.Graduate level students may not enroll.

**CSEC 3351 Database Design**
**Credits:** 3 (3-0-0)
Basic database design and introduction to structured query language (SQL). Includes instruction on creating user interface forms for a database. TSI Restriction(s): Reading, Math, and Writing. Graduate level students may not enroll.

**Prerequisites:** Grade of 'C' or better in each: MATH 1314 or equivalent, CSEC 1436 or CSCI 1436 or (CSCI 1336 and CSCI 1136).

**Restrictions:** Graduate level students may not enroll.

**CSEC 3366 Database Security**
**Credits:** 3 (3-0-0)
This course covers security attacks, threats, and mitigation techniques for securing modern database platforms and applications, such as SQL injection and data inference attacks. It also introduces database security architectures and secure database administration for Database Management Systems (DBMS). .

**Prerequisites:** Grade of 'C' or better in each: MATH 1314 or equivalent, CSEC 1436 or CSCI 1436 or (CSCI 1336 and CSCI 1136), and CSEC 3351 or CISA 3351.

**Restrictions:** Graduate level students may not enroll.

**CSEC 3385 Secure Software Engineering**
**Credits:** 3 (3-0-0)
This course covers secure software engineering processes and standards for building secure software applications. It discusses secure software life cycle development principles to include security in every phase of software engineering. It also explores security issues and vulnerabilities in software applications due to lack of secure software engineering process.

**Prerequisites:** A grade of C or better in each of : MATH 1314 or equivalent, CSEC 1436 or CSCI 1436 or (CSCI 1336 and CSCI 1136), CSEC 1437 or CSCI 1437 or (CSCI 1337 and CSCI 1137), CSEC 2306 or CISA 2306, CSEC 3321 or CISA 3321 or CSCI 3321.

**Restrictions:** Graduate level students may not enroll.

**CSEC 4101 Ethical Issues in Computing**
**Credit:** 1 (1-0-0)
In this course, students will identify the various ethical issues and values as it relates to future careers within their discipline. Students will study various cases and identify the ethical issues, and seek mechanisms for addressing and resolving the issues. Through mock debates, studying, writing and presenting professional ethical analysis studies, students will be prepared to understand and address the ethical issues within their discipline.

**Restrictions:** Enrollment limited to students with a semester level of Senior.Graduate level students may not enroll.

**CSEC 4322 Information Policy Assurance**
**Credits:** 3 (3-0-0)
This course explores information security policies. The course includes both sociological and psychological issues in policy implementation in general, a dialogue on information security specific policies, the structure of a policy, and the lifecycle of policy from creation to enactment. The course also exposes the student to issue specific policies in different domains of security to assist the students learn in context of real-life situations. TSI Restriction(s): Reading, Math, and Writing. Graduate level students may not enroll.

**Prerequisites:** Grade of 'C' or better in each: MATH 1314 or equivalent, CSEC 2306 or CISA 2306, CSEC 3321 or CISA 3321.

**Restrictions:** Graduate level students may not enroll.

**CSEC 4323 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. TSI Restriction(s): Reading, Math, and Writing. Graduate level students may not enroll.

**Prerequisites:** Grade of 'C' or better in each: MATH 1314 or equivalent, CSEC 2306 or CISA 2306, CSEC 3321 or CISA 3321.

**Restrictions:** Graduate level students may not enroll.

**CSEC 4324 Penetration Testing**
**Credits:** 3 (3-0-0)
Students will use penetration testing methods to assess, exploit, and report security vulnerabilities on web applications, Internet protocols and services, and other common software vulnerabilities and system configuration errors. The course will emphasize the ethical application of penetration testing methods and tools. TSI Restriction(s): Reading, Math, and Writing. Graduate level students may not enroll.

**Prerequisites:** Grade of 'C' or better in each: MATH 1314 or equivalent, CSEC 2306 or CISA 2306, CSEC 3321 or CISA 3321.

**Restrictions:** Graduate level students may not enroll.

**CSEC 4326 Security & Operation Practicum**
**Credits:** 3 (3-0-0)
This course combines the theoretical foundation of system security with hands-on practical application on real systems. Students will practice roles of network and system administrators and system architects from both security and business operations perspectives and examines ethical issues in computing. Meets College of Business Experiential Learning Requirements. TSI Restriction(s): Reading, Math, and Writing. Graduate level students may not enroll.

**Prerequisites:** Grade of 'C' or better in each: MATH 1314 or equivalent, CSEC 2306 or CISA 2306, CSEC 3321 or CISA 3321, CSEC 3325 or CISA 3325, CSEC 4324 or CISA 4324.

**Restrictions:** Graduate level students may not enroll.

**CSEC 4350 Security Research Practicum**
**Credits:** 3 (3-0-0)
This course provides real-world research and problem-solving experience on current advanced cyber security threats and attack vectors/scenarios in a range of cyber security research topics. Students will apply security mechanisms and research methodology to solve security issues. This course may be supplemented as an external industry internship in related cyber security area based on prior approval of the instructor and the Department Chair.

**Restrictions:** Graduate level students may not enroll.

**CSEC 4351 Internship in Cyber Security**
**Credits:** 3 (3-0-0)
An off-campus learning and hands-on experience allowing the acquisition and application of cyber security skills in an actual work or business setting. TSI Restriction(s): Reading, Math, and Writing

**Restrictions:** Graduate level students may not enroll.

**CSEC 4358 Senior Project and Seminar**
**Credits:** 3 (3-0-0)
This course will introduce the student to the concepts, principles, and applications of information systems technology in the business environment, including a study of organizational structure, management and personnel of a data center, and the planning, organizing, and control activities necessary for good management of the information systems resource. Students will also complete an information system development project. Meets College of Business Experiential Learning Requirements. TSI Restriction(s): Reading, Math, and Writing. Graduate level students may not enroll.

**Prerequisites:** Grade of C or better in each of: MATH 1314, CSEC 1436 or CSCI 1436 or (CSCI 1336 and CSCI 1136), CSEC 3309 or CISA 3309, CSEC 3351 or CISA 3351.

**Restrictions:** Enrollment is limited to students with a major in Cybersecurity.Graduate level students may not enroll.

**CSEC 4380 Applied Cryptosystems**
**Credits:** 3 (3-0-0)
This course begins with an overview of necessary background in algebra and number theory, private- and public-key cryptosystems, applied cryptography, and basic signature schemes. The course covers cryptographic implementation in software and web application programming. Security testing of cryptographic implementations will be introduced, including testing. The course will also cover construction of untraceable electronic cash on the net and quantum cryptography, and one or more of digital watermarking, fingerprinting, and steganography. TSI Restriction(s): Reading, Math, and Writing. Graduate level students may not enroll.

**Prerequisites:** Grade of 'C' or better in each: MATH 1314 or equivalent, CSEC 1436 or CSCI 1436 or (CSCI 1336 and CSCI 1136), CSEC 1437 or CSCI 1437 or (CSCI 1337 and CSCI 1137), CSEC 2336 or CSCI 2436 or (CSCI 2336 and CSCI 2136), CSEC 3309 or CISA 3309, CSEC 3321 or CISA 3321.

**Restrictions:** Graduate level students may not enroll.

**CSEC 4386 Cloud and Big Data Security**
**Credits:** 3 (3-0-0)
This course introduces concepts of cloud computing, its reference model, and Big Data applications in the context of security. It will cover knowledge on cloud architectures of major cloud providers, and big data applications and platforms including MapReduce, Hadoop. The course will focus on security risks and threats in cloud architectures and big data applications, and explore mitigation and countermeasures. It will also investigate the applicability of big data analytics to identify and mitigate cloud and big data security risks. TSI Restriction(s): Reading, Math, and Writing. Graduate level students may not enroll.

**Prerequisites:** Grade of 'C' or better in each: MATH 1314 or equivalent, CSEC 1436 or CSCI 1436 or (CSCI 1336 and CSCI 1136), CSEC 1437 or CSCI 1437 or (CSCI 1337 and CSCI 1137), CSEC 2436 or CSCI 2336 or (CSCI 2336 and CSCI 2136), CSEC 3309 or CISA 3309, CSEC 3321 or CISA 3321.

**Restrictions:** Graduate level students may not enroll.

**CSEC 4391 IoT Security**
**Credits:** 3 (3-0-0)
This course prepares students to securely develop and operate Internet of Things (IoT) devices and cyber-physical systems (CPS) with embedded software and firmware. The course covers concepts on IoT and CPS architectures and application domains. It examines specific security and privacy risks in IoT and CPS and their application domains, and enables students to learn and develop methods or countermeasures to address those risks and threats. TSI Restriction(s): Reading, Math, and Writing. Graduate level students may not enroll.

**Prerequisites:** Grade of 'C' or better in each: MATH 1314 or equivalent, CSEC 1436 or CSCI 1436 or (CSCI 1336 and CSCI 1136), CSEC 1437 or CSCI 1437 or (CSCI 1337 and CSCI 1137), CSEC 3309 or CISA 3309, and CSEC 3321 or CISA 3321.

**Restrictions:** Graduate level students may not enroll.

**CSEC 4392 Topics in Cyber Security**
**Credits:** 3 (3-0-0)
This course will explore emerging and advanced topics in cyber security area. The course may be repeated once for additional credit, based on a different cyber security topic or any other relevant topic covered in the course, with approval of the instructor and the Department Chair.

**Restrictions:** Graduate level students may not enroll.

**CSEC 4394 Cyber Intelligence**
**Credits:** 3 (3-0-0)
This course will integrate knowledge from introductory security courses with knowledge from data science and analytics. Major subjects include: Cyber operations and management, cyber defense and offense, malware analysis, and reverse engineering. The course will be built based on NIST NICE Cyber framework. TSI Restriction(s): Reading, Math, and Writing. Graduate level students may not enroll.

**Prerequisites:** Grade of 'C' or better in each: MATH 1314 or equivalent, CSEC 1436 or CSCI 1436 or (CSCI 1336 and CSCI 1136), CSEC 1437 or CSCI 1437 or (CSCI 1337 and CSCI 1137), CSEC 2336 or CSCI 2436 or (CSCI 2336 and CSCI 2136), CSEC 3309 or CISA 3309, CSEC 3321 or CISA 3321.

**Restrictions:** Graduate level students may not enroll.

**CSEC 4483 Advanced Penetration Testing**
**Credits:** 4 (4-0-0)
This course covers advanced penetration testing mechanisms and tools, such as ethical hacking tools. It will focus on advanced penetration testing tools to find vulnerabilities in applications, operating systems and network communication and APIs, etc. Students will analyze the impact of pre and post security event/incidents in a business environment.

**Prerequisites:** Grade of C or better in CSEC 1437 or CSCI 1437, CSEC 1360, CSEC 4324 or CISA 4324.

**Restrictions:** Enrollment is limited to students with a major in Cybersecurity.Graduate level students may not enroll.

**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:** Undergraduate level students may not enroll.

**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:** Undergraduate level students may not enroll.

**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:** Undergraduate level students may not enroll.

**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:** Undergraduate level students may not enroll.

**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:** Undergraduate level students may not enroll.

**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:** Undergraduate level students may not enroll.

**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:** Undergraduate level students may not enroll.

**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:** Undergraduate level students may not enroll.

**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:** Undergraduate level students may not enroll.

**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:** Undergraduate level students may not enroll.

**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:** Undergraduate level students may not enroll.

**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:** Undergraduate level students may not enroll.

**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:** Undergraduate level students may not enroll.

**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:** Undergraduate level students may not enroll.