CYBERSECURITY (CSEC)

CSEC 228 | LEGAL, ETHICAL AND SOCIAL ISSUES IN INFORMATION SECURITY (FORMERLY CNS 228) | 4 quarter hours
(Undergraduate)
This course is designed to acquaint students with electronic privacy, security and ethics. Students will gain an understanding of information ethics, existing and emerging cyber-laws, organizational liability issues, and explore several Codes of Ethics. Students will learn about real and potential security issues, steps that can be taken to create environments of trust, how to evaluate the strengths and weaknesses of a firm's information resource environment, and risk management and operation feasibility issues.

CSEC 320 | COMPUTER FORENSIC AND INCIDENT RESPONSE (FORMERLY CNS 320) | 4 quarter hours
(Undergraduate)
Introduction to the topics of computer forensic, computer crimes, response to security incidents, Cybercrime investigation and prosecution. Students will learn how an organization can setup a security response team, prepare for Security incidents and manage these incidents.
CSEC 378 or CSC 374 is a prerequisite for this class

CSEC 328 | FUNDAMENTALS OF IT RISK | 4 quarter hours
(Undergraduate)
This course describes the principles of IT risk management, responsibilities and accountability for IT risk, ways to develop risk awareness, and how to communicate risk scenarios, business impacts and key risk indicators. The course covers risk identification, evaluation, and response; students will have the opportunity to create a business-focused, process-oriented and measurement-driven risk response plan.

CSEC 340 | FUNDAMENTALS OF INFORMATION ASSURANCE (FORMERLY CNS 340) | 4 quarter hours
(Undergraduate)
This course is a survey of the fundamental elements of computer security and information assurance. Topics may include confidentiality, integrity, and availability; security policies; authentication; access control; risk management; threat and vulnerability assessment; common attack/defense methods; ethical issues.

CSEC 342 | CYBERSECURITY OPERATIONS (FORMERLY CNS 342) | 4 quarter hours
(Undergraduate)
The Cybersecurity Operations course presents the knowledge and skills needed for a Security Analyst in a typical Security Operations Center environment. The course covers the core security skills needed for monitoring, detecting, investigating, analyzing and responding to security events. Extensive laboratory exercises are included to apply knowledge learned in the lectures and allow the students to implement typical SOC tools. In addition to technologies, the course will also cover cybersecurity operations network principles, roles and responsibilities as well as the related technologies, tools, regulations and security frameworks.

CSEC 345 | HUMAN-CENTERED CYBERSECURITY (FORMERLY CNS 345) | 4 quarter hours
(Undergraduate)
A survey of behavioral theories relevant in cybersecurity context. Topics include economic theories of decision making, heuristics, biases, and bounded rationality, signal detection theory, mental models, social engineering, game theory, information search, and cognitive engineering. Students work on term paper describing potential application(s) of a theory of their choice in cybersecurity context. PREREQUISITE(S): IT 263 or CSC 242.

CSEC 348 | ONLINE MISINFORMATION AND DISINFORMATION OPERATIONS | 4 quarter hours
(Undergraduate)
A hands-on course in which students familiarize themselves with the concepts of information operations, dissemination of misinformation and disinformation online (e.g. social media platforms, Wikipedia, forums, chatrooms, etc.), fact checking, automated detection, evasion, and the lifecycle of alternative narratives. Antecedents, cognitive predispositions, and the history of misinformation and disinformation in human evolution as well as societies are also discussed. Students work on a misinformation labeling of social media posts for their final project.

CSEC 355 | PHYSICAL AND IT SECURITY CONVERGENCE (FORMERLY CNS 355) | 4 quarter hours
(Undergraduate)
This course introduces students to the fundamental processes associated with the Physical Security discipline. This course will present the convergence of IT Security and Corporate Physical Security, focusing on where convergence takes place - at the technology, process and function level. Students will look at real-world illustrations of implementation and analyze perceived efficiencies and cost-savings. This course is designed for students who desire to understand physical and IT security in the framework of Enterprise Risk Management.

CSEC 356 | APPLIED SOCIAL ENGINEERING | 4 quarter hours
(Undergraduate)
A hands-on course in which students investigate social engineering attacks in controlled lab environments and develop technical, policy, and risk management responses. Topics include: social engineering mechanics, principles of persuasion, preparation, traditional social engineering attacks and defenses, Ambient Tactical Deception (ATD), false information online, ethical aspects of social engineering, and automation/machine learning support for social engineering. Students work on an individual social engineering training scenario for their final project.

CSEC 366 | CRITICAL INFRASTRUCTURE AND CONTROL SYSTEMS CYBERSECURITY (FORMERLY CNS 366) | 4 quarter hours
(Undergraduate)
This course is an introduction to the cybersecurity challenges for control systems present in industry, homes and traditional businesses such as manufacturing. Topics covered include the design and setup of Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and Programmable Logic Controller (PLC) systems. As these systems are typically designed without any intrinsic security mechanism, we will study the challenges of protecting them and how to employ a defense-in-depth methodology to secure them. This class will focus on the security risks of critical infrastructure systems (such as Electrical, Pipelines, Water/Wastewater and transportation) and methods to protect them. PREREQUISITE(S): CSEC 340 or NET 377 or IT 263.

CSEC 378 | HOST BASED SECURITY (FORMERLY CNS 378) | 4 quarter hours
(Undergraduate)
Principles of host based security. Review of security methods used to ensure the confidentiality, integrity, and availability of the information stored on a host. The class will cover OS configuration, access control, anti-malware, public facing application security, host-based intrusion detection/prevention, host-based firewalls and audit & compliance. Course includes laboratory work with both the Linux and Windows operating systems.
NET 363 or CSC 374 is a prerequisite for this class.

CSEC 380 | ADVANCED CYBERSECURITY AUTOMATION (FORMERLY CNS 380) | 4 quarter hours
(Undergraduate)
This hands-on course will introduce students to real world exercises and scenarios. Students will create tools to perform automation, monitoring, red and blue team operations. Techniques will be applied to topics such as operating systems, infrastructure hardening, virtualization, sandboxing, incident response, and web applications.

CSEC 388 | SECURITY TESTING AND ASSESSMENT (FORMERLY CNS 388) | 4 quarter hours
(Undergraduate)
Vulnerability assessment and ethical security testing; review of ethical concerns and legal issues associated with security testing activities; study and analysis of the defensive mechanisms used to mitigate such threats. There will be extensive hands-on laboratory exercises.
CSEC 340 and CSEC 378 are prerequisites for this class.

CSEC 389 | CYBER DEFENSE EXERCISES AND ATTACK RESPONSES (FORMERLY CNS 389) | 4 quarter hours
(Undergraduate)
This is a hands-on, lab based applied security course in which students will work in teams to defend against cyber-attacks and implement services in a hostile cyber environment. Most activities will be derived from Cyber Dense and Cyber League competitions and will prepare students to participate and excel in these competitions. This course is open to all students, including students inexperienced in Cyber Defense competitions. Repeat enrollment is encouraged.
CSEC 340 and CSEC 378 are prerequisites for this class.

CSEC 390 | VULNERABILITY ASSESSMENT FOR COMMUNITY-BASED ORGANIZATIONS (FORMERLY CNS 390) | 4 quarter hours
(Undergraduate)
This service learning course prepares students with real-world experience by partnering with a non-profit, community-based organization to identify information security vulnerabilities and propose recommendations that improve the organization's security and privacy practices. Within the context of an assigned community-based organization, students will work in teams to conduct a vulnerability assessment; identify and propose cost-effective safeguards that may be administrative, technical, or physical; define a plan to test, monitor, and train system users on recommended security safeguards, and; document project deliverables for the organization's management. The course emphasizes hands-on exercises and student reflection on a community-based term project.

CSEC 394 | INFORMATION SYSTEMS SECURITY ENGINEERING I (FORMERLY CNS 394) | 4 quarter hours
(Undergraduate)
This course requires students to apply Information System Security Engineering methods and processes to design, document and implement comprehensive security infrastructures in realistic scenarios. Students will work in teams through the entire life cycle of a Security infrastructure project from needs discovery, threat assessment, architecture design, implementation, effectiveness assessment and auditing. The course is designed to span two quarters. In this first quarter, students will learn the Information Systems Security Engineering process and perform asset identification, threat assessment and system requirement specification.
NET 377 and NET 379 and CSEC 388 are prerequisites for this course.

CSEC 395 | INFORMATION SYSTEMS SECURITY ENGINEERING II (FORMERLY CNS 395) | 4 quarter hours
(Undergraduate)
This senior project capstone course requires students to apply Information System Security Engineering methods and processes to perform the design and implementation of Information Systems Security infrastructures. The human and sociological impacts of Information Security will be studied with a particular focus on privacy issues, ethical use of Security tools and cultural and legal difference that exist in a globally connected but diverse world.
CSEC 394 is a prerequisite for this class.

CSEC 397 | TOPICS IN COMPUTER, INFORMATION AND NETWORK SECURITY FORMERLY CNS 397) | 1-4 quarter hours
(Undergraduate)
May be repeated for credit. (1 quarter hour)

CSEC 399 | INDEPENDENT STUDY (FORMERLY CNS 399) | 1-8 quarter hours
(Undergraduate)
Variable credit. PREREQUISITE(S): Consent of dean. (variable credit)

CSEC 418 | INTRODUCTION TO HOST SECURITY (FORMERLY CNS 418) | 4 quarter hours
(Graduate)
Principles of host based security. Review of security methods used to ensure the confidentiality, integrity, and availability of the information stored on a host. The class will cover OS configuration, access control, anti-malware, public facing application security, host-based intrusion detection/prevention, host-based firewalls and audit & compliance. Course includes laboratory work with both the Linux and Windows operating systems.
NET 405 is a prerequisite for this class.

CSEC 428 | IT RISK MANAGEMENT | 4 quarter hours
(Graduate)
This course provides an in-depth view of IT-related business risk management and the methodology that includes risk identification, evaluation and response. The course describes the principles of IT risk management, responsibilities and accountability for IT risk, how to build risk awareness, and how to communicate risk scenarios, business impacts and key risk indicators. Students will have the opportunity to create a business-focused, process-oriented and measurement-driven risk response plan; the course will also prepare students for the IT Risk Fundamentals Certificate offered by ISACA.

CSEC 440 | INFORMATION SECURITY MANAGEMENT (FORMERLY CNS 440) | 4 quarter hours
(Graduate)
Survey of information security management as it applies to information systems analysis, design, and operations. Managing information assets and the security infrastructure. Emphasis on managing security-related risk, as well as the process of developing, implementing, and maintaining organizational policies, standards, procedures, and guidelines. Identifying and evaluating information assets, threats, and vulnerabilities. Quantitative and qualitative risk analysis, risk mitigation, residual risk, and risk treatment as they relate to information security. Topics include information security vulnerabilities, threats, and risk management; security policies and standards; security audits; access controls; network perimeter protection, data protection; physical security; security education training and awareness. Introduction to compliance, as well as the CISSP domains.

CSEC 445 | HUMAN-CENTERED CYBERSECURITY (FORMERLY CNS 445) | 4 quarter hours
(Graduate)
Application of behavioral theories in cybersecurity context. Topics include economic theories of decision making, heuristics, biases, and bounded rationality, signal detection theory, mental models, social engineering, game theory, information search, and cognitive engineering. Students work on an individual project applying one of these theories to a practical cybersecurity scenario of their choice.

CSEC 446 | SECURE DESIGN (FORMERLY CNS 446) | 4 quarter hours
(Graduate)
Secure design is a cross-disciplinary approach to cybersecurity and user-centered design. The course includes hands-on, interactive activities focused on secure designs for Internet-of-Things (IoT) technologies. Topics include: principles of visual design, user-centered design, mental models, heuristics, bounded rationality, applied cybersecurity, prototyping, and usability testing. Students will work on a class long project that will employ the principles of secure design to develop a secure yet usable prototype of an IoT device.

CSEC 448 | ONLINE MISINFORMATION AND DISINFORMATION OPERATIONS | 4 quarter hours
(Graduate)
A hands-on course in which students familiarize themselves with the concepts of information operations, dissemination of misinformation and disinformation online (e.g. social media platforms, Wikipedia, forums, chatrooms, etc.), fact checking, automated detection, evasion, and the lifecycle of alternative narratives. Antecedents, cognitive predispositions, and the history of misinformation and disinformation in human evolution as well as societies are also discussed. Students work on the design of an experimental social media platform for socially calibrated misinformation and disinformation containment for their final project.

CSEC 450 | DIGITAL FORENSIC TECHNIQUES (FORMERLY CNS 450) | 4 quarter hours
(Graduate)
This course focuses on the forensic acquisition, analysis and presentation of data from computer systems. This course covers: preservation and interpretation of evidence; forensic imaging; file systems and data recovery; Windows registry forensics; internet history and social media analysis; mobile device forensics; timeline analysis; incident response and writing expert reports and testimony.
CSC 407 or CSEC 418 is a prerequisite for this class.

CSEC 455 | PHYSICAL AND IT SECURITY CONVERGENCE (FORMERLY CNS 455) | 4 quarter hours
(Graduate)
This course introduces students to the fundamental processes associated with the Physical Security discipline. This course will present the convergence of IT Security and Corporate Physical Security, focusing on where convergence takes place - at the technology, process and function level. Students will look at real-world illustrations of implementation and analyze perceived efficiencies and cost-savings. This course is designed for students who desire to understand physical and IT security in the framework of Enterprise Risk Management.

CSEC 456 | APPLIED SOCIAL ENGINEERING | 4 quarter hours
(Graduate)
A hands-on course in which students investigate social engineering attacks in controlled lab environments and develop technical, policy, and risk management responses. Topics include: social engineering mechanics, principles of persuasion, preparation, traditional social engineering attacks and defenses, Ambient Tactical Deception (ATD), false information online, ethical aspects of social engineering, and automation/machine learning support for social engineering. Students work on an individual design, exploit, detection, prevention, and deterrence in a practical social engineering scenario of their choice for their final project. Students work on designing, implementing, and testing an automation/machine learning tool for detecting social engineering on Twitter for their final project.

CSEC 466 | CRITICAL INFRASTRUCTURE AND CONTROL SYSTEMS CYBERSECURITY (FORMERLY CNS 466) | 4 quarter hours
(Graduate)
This course is an introduction to the cybersecurity challenges for control systems present in industry, homes and traditional businesses such as manufacturing. Topics covered include the design and setup of Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and Programmable Logic Controller (PLC) systems. As these systems are typically designed without any intrinsic security mechanism, we will study the challenges of protecting them and how to employ a defense-in-depth methodology to secure them. This class will focus on the security risks of critical infrastructure systems (such as Electrical, Pipelines, Water/Wastewater and transportation) and methods to protect them.
CSEC 440 or NET 477 is a prerequisite for this class.

CSEC 477 | GOVERNANCE POLICIES IN INFORMATION ASSURANCE (FORMERLY CNS 477) | 4 quarter hours
(Graduate)
This course focuses on assessment of business risks arising from information security and privacy issues, as well as the creation and implementation of policies that ensure compliance with laws and industry standards. It is a complement to IS 482, which focuses on the legal standards to which people and organizations are held under laws and regulations that concern computing and information technology. Legal issues arising under information security and control frameworks, such as COBIT and IS017799, are considered. Topics include privacy laws, payment card industry standards, information security measures mandated by select federal statues (e.g., HIPAA, Gramm-Leach-Bliley and Sarbanes-Oxley), data breach notification, governance and policy development, e-discovery, contracts, intellectual property, and security risk assessments.
CSEC 440 is a prerequisite for this class

CSEC 480 | CYBERSECURITY AUTOMATION OPERATIONS | 4 quarter hours
(Graduate)
This intermediate course will build upon basic programming and cybersecurity knowledge to enable students to combine programming with real-world cybersecurity skills. Students will create scripts to perform automation, monitoring, red and blue team operations. Scripting will be applied to topics such as operating systems, networking, incident response, and web applications. Students will also learn about revision control, automation deployment options, and containerization.
CSC 401 and (CSEC 418 or CSC 407) are prerequisites for this class.

CSEC 488 | SECURITY TESTING AND ASSESSMENT (FORMERLY CNS 488) | 4 quarter hours
(Graduate)
Methodologies and tools for performing vulnerability testing; management of security testing initiatives and activities; review of the different types of assessments, legal issues, ethical concerns. Defensive mechanisms to mitigate the risks illustrated by the assessment using Defense-In-Depth architectures. Concepts illustrated using hands-on lab exercises.
CSEC 440 and CSEC 418 are prerequisites for this class.

CSEC 489 | ADVANCED CYBER ATTACK RESPONSES AND DEFENSES (FORMERLY CNS 489) | 4 quarter hours
(Graduate)
This lab-based applied security course introduces students to advanced cyber defense and cyber-attack response. Students manage an organize teams to defend against cyber-attacks and implement services in a hostile cyber environment. Most activities will be derived from Cyber Defense and Cyber League competitions and will prepare students to participate and excel in these competitions. This course is open to all students, including students inexperienced in Cyber Defense competitions. Repeat enrollment is encouraged.
CSEC 440 and CSEC 418 are prerequisites for this class.

CSEC 490 | INFORMATION SECURITY RISK ASSESSMENT FOR NON-PROFIT ORGANIZATIONS (FORMERLY CNS 490) | 4 quarter hours
(Graduate)
Students taking this course will gain real-world experience by partnering with a non-profit, community-based organization to assess information security needs and propose recommendations that improve the organization's security and privacy practices. Within the context of an assigned non-profit organization, students will work in teams to conduct a security risk assessment using industry standards as guidance; write a formal risk assessment report for the organization's management; identify and propose cost-effective security safeguards that may consist of security policies, technologies, or procedures; define a plan to test, monitor, and train system users on recommended security safeguards.
CSEC 440 is a prerequisite for this class

CSEC 533 | ENTERPRISE SECURITY INFRASTRUCTURE CONTROLS AND REGULATORY COMPLIANCE (FORMERLY CNS 533) | 4 quarter hours
(Graduate)
Design, implementation, support and management of control methods in enterprise environments. Focus is on how these controls can help organizations achieve regulatory compliance. Review of Sarbanes-Oxley and its impact on IT systems. Detailed study of how risk assessment methods, information security program management and ERP systems can be used to fulfill regulatory and legal requirements. Control Objectives for Information and related Technology (COBIT) guidelines and best practices for SOX compliance. Security management standards (ISO 17799, BS 7799 and ISO 27001) .
CSEC 440 is a prerequisite for this class

CSEC 587 | INFORMATION SECURITY GOVERNANCE (FORMERLY CNS 587) | 4 quarter hours
(Graduate)
In this course, students apply their knowledge of information security and regulatory compliance to analysis and evaluation of governance, risk management, and compliance problems. Students will learn the meaning of IT governance by examining the differences between governance and management; gaining hands-on application of industry governance frameworks; evaluating an information security program; defining incidence response policy; assessing risk; and defining regulatory compliance strategy. Students will discover how good information security governance adds value to an organization.
CNS 477 and (IS 444 or CNS 490 or CNS 533 or CSC 439 or NET 577) are prerequisites for this class.

CSEC 594 | COMPUTER INFORMATION AND NETWORK SECURITY CAPSTONE (FORMERLY CNS 594) | 4 quarter hours
(Graduate)
Design, setup and configuration of realistic enterprise computing and networking environments. Securing the infrastructure and integration of different services and technology in efficient, secured and redundant manners. Technologies will include: open-source and commercial products, firewalls, Virtual Private Networks (VPNs), authentication systems, Intrusion Detection Systems (IDS), advanced routing mechanisms (OSPF, BGP, IS-IS), highly redundant and robust networking.
NET 477 or CSEC 533 is a prerequisite for this class.

CSEC 597 | TOPICS IN COMPUTER INFORMATION AND NETWORK SECURITY (FORMERLY CNS 597) | 1-4 quarter hours
(Graduate)
Specific topics will be selected by the instructor and may vary with each quarter. Can be repeated for credit. Variable credit. PREREQUISITE(S): For specific prerequisites, see syllabus or consult course instructor. (variable credit)

CSEC 599 | INDEPENDENT STUDY (FORMERLY CNS 599) | 1-4 quarter hours
(Graduate)
Independent study supervised by an instructor. Independent study form required. Can be repeated for credit. Variable Credit. PREREQUISITE(S): None. (variable credit)