CIS: Computer Science and Information Systems Courses

Courses

CIS 2530 Introduction to Cybersecurity
College of Sci and Engineering, Department of Cybersecurity & Info Tech

3 sh (may not be repeated for credit)

This course introduces students to cybersecurity. It provides information related to cyber threats as well as the basic security design and information assurance fundamentals. In addition the course covers information assurance controlling laws and guidelines. Meets General Education requirement in Social Sciences.

CIS 3385 Introduction to Digital Forensics
College of Sci and Engineering, Department of Cybersecurity & Info Tech

3 sh (may not be repeated for credit)

Explores methodologies and techniques for maintaining integrity of forensic evidence. Uses popular forensics tools and provides specific guidance on the investigation process of cases relating to law and technology. Topics include representation, preservation and recovery of data from multiple sources, and legal issues unique to the digital forensics investigation process. Students will collect, examine, analyze and prepare detailed reports showing the relevance of digital evidence to cases.

CIS 3949 Cooperative Education
College of Sci and Engineering, Department of Cybersecurity & Info Tech

1-2 sh (may be repeated for up to 4 sh of credit)

Alternating full-time or consecutive parallel terms of practical experience in the intended field. Reinforcing academic preparation; confirming educational and career goals; personal and professional development; early start in career; earnings toward self-support; improved employability. (See program description under Cooperative Education). Graded on satisfactory/unsatisfactory basis only. Permission of director of Cooperative Education is required.

CIS 4221 Ethical Hacking and Penetration Testing
College of Sci and Engineering, Department of Cybersecurity & Info Tech

3 sh (may not be repeated for credit)
Prerequisite: (COP 3530 OR COP 3022) AND (CNT 4007)

This course provides a understanding of how to effectively protect computer networks. Students will learn the tools and penetration testing methodologies used by ethical hackers. The tools and methodology will focus on gathering information and identifying flaws and vulnerabilities in documentation, software and computer systems, and exploiting those flaws. In addition, the course provides a thorough discussion of what and who an ethical hacker is and how important they are in protecting corporate and government data from cyber attacks. Students will be provided with an overview of computer crime laws. This course is offered concurrently with CIS 5396; graduate students will be assigned additional work. Credit cannot be received in both CIS 4385 and CIS 5396.

CIS 4325 System Analysis and Design
College of Sci and Engineering, Department of Cybersecurity & Info Tech

3 sh (may not be repeated for credit)
Prerequisite: (CNT 3004 OR COP 4634 OR CNT 4007) AND (COP 4710) AND (COP 2253 OR COP 2334)

This course is designed to explain the techniques used in the information system development process. It introduces students to the principles and practices of systems analysis and design methods, focusing on planning, designing, implementing, testing, and securing an information system. Students will apply concepts from the class to provide solutions for a specific organizational function or process. Data modeling and process modeling are discussed in this course.

CIS 4361 Information Technology Security
College of Sci and Engineering, Department of Cybersecurity & Info Tech

3 sh (may not be repeated for credit)
Prerequisite: COP 2253 OR COP 2334 OR COP 2830

This course provides an overview of security challenges and strategies of countermeasure in the information systems environment. Topics include definition of terms, concepts, elements, and goals incorporating industry standards and practices with a focus on confidentiality, availability, and integrity aspects of information systems.

CIS 4368 Introduction to Database Security
College of Sci and Engineering, Department of Cybersecurity & Info Tech

3 sh (may not be repeated for credit)
Prerequisite: COP 4710

The Database Security course follows guidelines set forth by the National Security Agency Centers of Academic Excellence in Information Assurance and Cyber Defense. This course is considered a core knowledge unit for institutions to be considered a Center of Academic Excellence. Database Security is designed to teach students how database systems are used, managed, and issues associated with protecting the associated data assets. This undergraduate course is a requirement for the B.S. in Cybersecurity and will be an elective for all other undergraduate Computer Science and Information Technology programs.

CIS 4383 Introduction to Cyber Investigations
College of Sci and Engineering, Department of Cybersecurity & Info Tech

3 sh (may not be repeated for credit)
Prerequisite: CNT 3112 OR CNT 4007

The course introduces students to incident management, response, determination of incidents, and their associated frameworks. Students will use manual and automated tools to understand how incidents are detected and identified and recovery is performed using existing methodologies and frameworks.

CIS 4592 Capstone Project
College of Sci and Engineering, Department of Computer Science

3 sh (may not be repeated for credit)
Prerequisite: (CEN 3031) AND (COP 4534 OR CEN 4078) AND (COP 4634 OR COP 4610)

This course requires students to apply their skills in design, implementation, and evaluation of a software product addressing a complex, real-world problem. The course reinforces software engineering concepts and skills from previous coursework, focusing on best practices and methods for building software. Students will work as teams to develop a project plan, multiple prototypes, and a final software system for the project topic. Students will be required to prepare a final presentation on their project and a report that describes their achievements and provides a critical assessment of professional and ethical issues as well as their work and final product.

CIS 4595 Capstone Project
College of Sci and Engineering, Department of Cybersecurity & Info Tech

3 sh (may not be repeated for credit)
Prerequisite: (CNT 4403 OR CEN 3032) AND ((CEN 4078 AND COP 4610 AND COP 4710))

This course brings together students from different computing and security disciplines to solve complex, real-world problems in teams. Students develop, secure, and analyze computing systems applying the skills they have acquired in their respective majors. They develop and deliver relevant artifacts such as requirements, design, test, and security plans, as well as user documentation for those systems. Teams shall focus on the use of modern tools for collaboration, communication, and project management throughout the duration of this course. Students produce presentations and individual project evaluations. Ethical and professional issues will be addressed in the context of the project.

CIS 4905 Directed Study
College of Sci and Engineering, Department of Cybersecurity & Info Tech

1-12 sh (may be repeated indefinitely for credit)

CIS 4941 Computer Science Internship
College of Sci and Engineering, Department of Computer Science

1-3 sh (may not be repeated for credit)

Supervised field practicum in computer-related position. May include activities in computer programming, database administration, web-development, systems administration, network security, etc. Graded on satisfactory / unsatisfactory basis only. Juniors or seniors with minimum cumulative GPA of 3.00 will be eligible. Permission is required.

CIS 4947 Internship/Practicum in Information Technology
College of Sci and Engineering, Department of Cybersecurity & Info Tech

1-3 sh (may be repeated for up to 6 sh of credit)

Practical and significant Information Technology professional work experience under approved industrial supervision.

CIS 5396 Ethical Hacking and Penetration Testing
College of Sci and Engineering, Department of Cybersecurity & Info Tech

3 sh (may not be repeated for credit)
Prerequisite: CIS 5775

This course provides an understanding of how to effectively protect computer networks. Students will learn the tools and penetration testing methodologies used by ethical hackers. The tools and methodology will focus on gathering information and identifying flaws and vulnerabilities in documentation, software and computer systems and exploiting those flaws. In addition, the course provides a thorough discussion of what and who an ethical hacker is and how important they are in protecting corporate and government data from cyber attacks. Students will be provided with an overview of computer crime laws. Offered concurrently with CIS 4221; graduate students will be assigned additional work. Credit may not be received in both CIS 5396 and CIS 4221.

CIS 5775 Cybersecurity Principles
College of Sci and Engineering, Department of Cybersecurity & Info Tech

3 sh (may not be repeated for credit)

This course introduces students to topics in cybersecurity. It provides information related to threat models, vulnerability analysis, and security-policy formation and enforcement. In addition, the course covers information assurance controlling laws and guidelines as well as introduces students to broad topics in network and system security, Internet services, and digital forensics.

CIS 5905 Directed Study
College of Sci and Engineering, Department of Cybersecurity & Info Tech

1-12 sh (may be repeated indefinitely for credit)

CIS 6084 Cloud Computing Architecture and Security
College of Sci and Engineering, Department of Cybersecurity & Info Tech

3 sh (may not be repeated for credit)

This course provides students with the necessary knowledge and skills of cloud computing architecture and security. Students identify and evaluate cloud computing resources and services. Also, this course focuses on security issues and countermeasures. Additional topics vary but may include access control, identity access management, compliance, and trustworthy computing.

CIS 6376 Database Security
College of Sci and Engineering, Department of Cybersecurity & Info Tech

3 sh (may not be repeated for credit)
Prerequisite: COP 5725

Database Security is designed to teach students how database systems are used, managed, and issues associated with protecting the associated data assets are resolved. This course will cover various methods to ensure information confidentiality, integrity, and availability on various data storage systems. This graduate course is an elective for graduate Cybersecurity and Information Technology programs.

CIS 6394 Digital Forensics
College of Sci and Engineering, Department of Cybersecurity & Info Tech

3 sh (may not be repeated for credit)

This course will provide a solid foundation for performing a digital forensic examination; introduces tools and techniques required for conducting a forensic analysis on systems and data pertaining to evidences in civil, criminal or administrative cases. It introduces systematic problem-solving techniques and applies them to digital investigations. The techniques directly correlate to methods used to recover/restore data for various requirements, ranging from litigation to fraud-based investigations.

CIS 6511 Enterprise Information Technology Risk Management
College of Sci and Engineering, Department of Cybersecurity & Info Tech

3 sh (may not be repeated for credit)

This course introduces the risks that may emerge in enterprises. Students follow a holistic approach to applying well defined best practices in information systems risk management. This course provides the necessary skills and knowledge to evaluate, plan, mitigate, and protect information infrastructure and assets. Case studies may be used to demonstrate the issues and challenges in risk management.

CIS 6625 Data Security
College of Sci and Engineering, Department of Cybersecurity & Info Tech

3 sh (may not be repeated for credit)
Prerequisite: COP 5725

This course covers concepts of Data Security from a data centric perspective. Challenges faced by today's systems will be studied and the future of data security will be discussed. This course may require completion of graduate foundations courses in computer programming or the equivalent undergraduate coursework if a student has insufficient academic or professional experience in computer science.

CIS 6710 Trends in Information Technology
College of Sci and Engineering, Department of Cybersecurity & Info Tech

3 sh (may not be repeated for credit)

This course explores and leverages the latest technologies to solve existing business-related IT problems and proposes effective and efficient IT solutions. Emphasis will be given to the way technologies create competitive edge and solutions for various industries. Students will evaluate different options and provide the rationale for problem-solving alternatives related to system performance, resources, communication, and security.

CIS 6905 Directed Study
College of Sci and Engineering, Department of Cybersecurity & Info Tech

1-12 sh (may be repeated indefinitely for credit)

CIS 6950 Information Technology Capstone
College of Sci and Engineering, Department of Cybersecurity & Info Tech

3 sh (may not be repeated for credit)
Prerequisite: Completion of 18 hours of college course work is required prior to taking this course.

Students enrolled in the MSIT degree program are required to complete a three-credit hour, capstone project. Students will work in consultation with their instructor and an identified industry host to identify and complete a complex project related to their program of study. Students synthesize and apply knowledge developed during the academic program to identify, propose, and develop solutions to meet the complex networking needs of the host organization. Students must complete 18 graduate hours and obtain department permission to enroll.

CIS 6971 Thesis
College of Sci and Engineering, Department of Computer Science

1-6 sh (may be repeated for up to 12 sh of credit)

Graded on satisfactory / unsatisfactory basis only. Permission is required.