

CIS: Computer Science And Information Systems Courses

Courses

CIS 2352 Introduction to Ethical Hacking
3 sh (may not be repeated for credit)
Prerequisite: CTS 1120

This course provides a basic understanding of how to effectively protect computer networks by understanding how a system can be exploited. The course provides a discussion of what and who an ethical hacker is and how important they are in protecting corporate and government data from cyber-attacks as well as an overview of computer crime laws. Students will be provided a basic overview of tools and penetration testing methodologies used by ethical hackers to gathering information, identify flaws and vulnerabilities, and exploit those flaws.

CIS 2530 Introduction to Cybersecurity
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 Natural Sciences.

CIS 3325 Information Technology Infrastructure Analysis and Recommendation
3 sh (may not be repeated for credit)
Prerequisite: (COP 2253 OR COP 2334) AND (CGS 2920)

Students will develop the knowledge, skills and abilities necessary to analyze technology infrastructure needs of various types and sizes of organizations and provide appropriate solution recommendations to solve complex problems.

CIS 3512 Software Documentation
3 sh (may not be repeated for credit)
Prerequisite: ENC 1102

Introduction to major concepts of software documentation. Emphasis on construction of software system artifacts that support team development and evolution of software systems (e.g., memos, letters, project proposals, progress reports, requirements, specifications, design, test plans, test reports, project reports). MLA, APA, and LaTeX publication standards will be applied. Open to all majors Meets Gordon Rule Writing Requirement.

CIS 3949 Cooperative Education
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 4361C IT Security
3 sh (may not be repeated for credit)
Prerequisite: COP 2253 OR COP 2830

Introduction to skills, knowledge, techniques, and tools required by information-technology security professionals. Topics include security and risk management, physical security, access control, cryptography, security architecture and design, security for networks and telecommunications, application security, and legal considerations.

CIS 4368 Introduction to Database Security
3 sh (may not be repeated for credit)
Prerequisite: COP 4710

The Database Security course follows guidelines set forth by the National Security Agency/Department of Homeland Security 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 programs. Prerequisites: COP 4710, minimum grade of C-.

CIS 4385 Ethical Hacking and Penetration Testing
3 sh (may not be repeated for credit)
Prerequisite: (COP 3022 OR COP 3530) 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 4592 Capstone Project
3 sh (may not be repeated for credit)
Prerequisite: CEN 3031 AND COP 4534 AND COP 4634

This course follows up on Software Engineering I requiring students to apply the developed skills to design, implement, and evaluate a software product that addresses a complex, real-world problem. The course provides additional software engineering concepts and skills that students learned in Software Engineering I focusing on best practices and methods for building software. Students will work individually or 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 their work and final product.

CIS 4595 Capstone Systems Project

3 sh (may not be repeated for credit)

Prerequisite: (CNT 4403 OR CEN 3032) AND ((COP 4610 AND COP 4710))

Develop a software system for a real-world client while working in small teams. Develop and deliver relevant artifacts such as a project proposal, design, test plan, code, user's manual, and project log with metrics as the software system evolves throughout the course. A final presentation and evaluation of the project experience will be prepared.

CIS 4905 Directed Study

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

CIS 4941 Computer Science Internship

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

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. Graded on a satisfactory / unsatisfactory basis only.

CIS 5396 Ethical Hacking and Penetration Testing

3 sh (may not be repeated for credit)

Prerequisite: CDA 6415 AND COP 6025

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. Offered concurrently with CIS 4385;graduate students will be assigned additional work. Credit may not be received in both CIS 5396 and CIS 4385.

CIS 5905 Directed Study

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

CIS 6376 Database Security

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. This course will cover various methods to ensure information confidentiality, integrity and availability on an assortment of data storage systems. This graduate course is a requirement for the M.S.A. in Cyber Security and will be an elective for all other graduate Computer Science programs. Prerequisites: COP 5725 minimum grade of C.

CIS 6379 Applied Information Security

3 sh (may not be repeated for credit)

This course covers a variety of topics which range from information security fundamentals to the management and planning aspects of information security. Students in this course will learn to design and create information security policies, disaster recovery and risk analysis & mitigation plans. Students will also learn about security models and various physical and technical security controls.

CIS 6394 Digital Forensics

3 sh (may not be repeated for credit)

This course will cover basic concepts and 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 theories directly correlate to methods used to recover/restore data for various requirements, ranging from litigation to fraud based investigations.

CIS 6415 Advanced Computer Systems and Networks

3 sh (may not be repeated for credit)

Examines current advancements in computer hardware, operating systems and networks. their relation to each other, and programming practices that takes advantage of them. Topics include pipelined, hyperthreaded, multicore and multiprocessor architectures, scheduling methods, distributed and real-time systems, high-speed networks, routing, congestion and flow control, and quality of service.

CIS 6905 Directed Study

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

CIS 6971 Thesis

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

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