

# CYBER SECURITY (CYBR)

---

## CYBR 1400 Ethical Behavior in Computing

[4 credit hours]

This course will teach the ethical dilemmas for computer use, the software engineering code of ethics and professional practice, and basic rules for computer ethics. The course will focus on the commitment software engineers have to the public, client and employer, product, judgement, management, profession, colleagues, and self.

**Term Offered:** Spring, Fall

## CYBR 2000 Cyber Law & Compliance, Intro to Cryptoanalysis & Generic Attacks

[4 credit hours]

An in-depth examination of the law dealing with computers and the Internet, including such issues as intellectual property, electronic commerce, information privacy, freedom of expression, cyber crime and jurisdiction. Included are detailed analyses of significant legal case studies plus review of applicable federal and state legislation. The course addresses key concepts in building and breaking ciphers by making, testing, securing and cracking programs that encrypt text with classical ciphers like the transposition cipher, Vigenère cipher, etc. Students will learn about major topics in crypt analysis. Also, students will study and analyze attack methods and algorithms in crypt analysis.

**Prerequisites:** CSET 1100 with a minimum grade of D-

**Term Offered:** Spring, Fall

## CYBR 2410 Digital Forensics

[3 credit hours]

This course trains students on the procedures and techniques used to identify, extract, validate, document and preserve electronic evidence. Students completing this course will be familiar with the core computer science theory and practical skills necessary to perform basic computer forensic investigations, understand the role of technology in investigating computer-based crime, and be prepared to deal with investigative bodies at a basic level.

**Prerequisites:** CYBR 2000 with a minimum grade of D-

**Term Offered:** Spring, Fall

## CYBR 3200 Client-Server Security Models

[3 credit hours]

This course trains students to systematically identify vulnerabilities, analyzing their occurrence, make corrective action options, evaluate from the aspect of the client/server model, and discuss and implement prescriptive software security designs.

**Prerequisites:** CYBR 2410 with a minimum grade of D-

**Term Offered:** Spring, Fall

## CYBR 3350 Managing Security Projects

[3 credit hours]

This course trains students on best practices on how institutions and organizations manage information risk through risk assessment practices and procedures.

**Prerequisites:** CYBR 2410 with a minimum grade of D-

**Term Offered:** Spring, Fall

## CYBR 4200 Software Assurance

[4 credit hours]

Practices for ensuring quality through the software process. Topics include requirements elicitation, analysis and documentation, testing, and quality assurance management.

**Prerequisites:** CSET 3600 with a minimum grade of D-

**Term Offered:** Spring, Fall

## CYBR 4500 Risk Vulnerability Analysis

[3 credit hours]

This course teaches risk vulnerabilities in an information network. Topics include administrating Linux and Microsoft servers together to provide infrastructure services to mixed clients. Topics covered are DNS; DHCP; file, web, mail, and directory security of these services; and best practices for combining and mixing server platforms in an enterprise environment.

**Prerequisites:** INFS 3400 with a minimum grade of D-

**Term Offered:** Spring, Fall