Course Outline

2026-2027 Catalog

CSCI 17 - Introduction to Cybersecurity/Security+

Catalog Description

Transfer Status: CSU

Unit(s): 3.00

Lecture: 34.00 Contact hours/68.00 Out of class hours/102.00 Total hours/2.00 Unit(s)

Lab: 51.00 Contact hours/0.00 Out of class hours/51.00 Total hours/1.00 Unit(s)

Total: 85.00 Contact hours/68.00 Out of class hours/153.00 Total hours/3.00 Unit(s)

Course Description: An introduction to the fundamental principles and topics of Information Technology Security and Risk Management at the organizational level. It addresses hardware, software, processes, communications, applications, and policies and procedures with respect to organizational Cybersecurity and Risk Management. Preparation for the CompTIA Security+ certification exams. (C-ID ITIS 160).

Objectives

Upon successful completion of this course, the student should be able to:

1. Describe the fundamental principles of information systems security.
2. Define the concepts of threat, evaluation of assets, information assets, physical, operational, and information security and how they are related.
3. Evaluate the need for the careful design of a secure organizational information infrastructure.
4. Perform risk analysis and risk management.
5. Determine both technical and administrative mitigation approaches.
6. Explain the need for a comprehensive security model and its implications for the security manager or Chief Security Officer (CSO).
7. Create and maintain a comprehensive security model.
8. Apply security technologies.
9. Define basic cryptography, its implementation considerations, and key management.
10. Design and guide the development of an organization's security policy.
11. Determine appropriate strategies to assure confidentiality, integrity, and availability of information.
12. Apply risk management techniques to manage risk, reduce vulnerabilities, threats, and apply appropriate safeguards/controls.

Course Content

Topic Titles / Suggested Time Topic

Lecture

Topics	Lec Hrs
Introduction to Information Systems Security	2.00
Malware and Social Engineering Attacks	3.00
Application and Network Attacks	3.00
Vulnerability Assessment and Mitigating Attacks	3.00
Host, Application, and Data Security	3.00
Network Security	3.00
Administering a Secure Network	3.00
Wireless Network Security	3.00
Authentication and Account Management	3.00
Access Control Fundamentals	2.00
Basic Cryptography	1.00
Advanced Cryptography	1.00
Business Continuity	2.00
Risk Mitigation	2.00
Total Hours:	**34.00**

Lab

Topics	Lab Hrs
Introduction to Information Systems Security	2.00
Malware and Social Engineering Attack	4.00
Application and Network Attacks	4.00
Vulnerability Assessment and Mitigating Attacks	4.00

Topics	Lab Hrs
Host, Application, and Data Security	4.00
Network Security	3.00
Administering a Secure Network	5.00
Wireless Network Security	5.00
Access Control Fundamentals	4.00
Authentication and Account Management	4.00
Basic Cryptography	3.00
Advanced Cryptography	3.00
Business Continuity	3.00
Risk Mitigation	3.00
Total Hours:	**51.00**

Methods of Instruction

A. Demonstrations
B. Homework: Students are required to complete two hours of outside-of-class homework for each hour of lecture
C. Lecture
D. Multimedia Presentations

Methods of Evaluation

A. Exams/Tests
B. Quizzes
C. Oral Presentation
D. Lab Projects
E. Essays and research papers

Examples of Assignments

Reading Assignments

1. Read the article provided by the instructor about how a NYC data center dealt with Hurricane Sandy. Write a few paragraphs about what you learned from their preparation and be prepared to discuss the article in class.
2. You have a single domain website and want to secure your online sales transactions, and you also want it to be obvious to your buyers that it is a secure site. Read the documentation about the cost and services provided by two different trusted commercial CAs. Compare and contrast the reputation for an EV SSL Certificate. Submit an outline of your findings to your instructor.

Writing Assignments

1. Compare a disaster recovery plan and a business continuity plan. Compare and contrast the value of each in a half-page description.
2. Write a one-page acceptable use policy for employees of an enterprise level company. Include an explanation of security and malware risks to the company network and what users can do to help avoid infection.

Out-of-Class Assignments

1. On your home computer, download and install an encryption application like GPG. Experiment with it and be prepared to discuss your findings with the class.
2. Research a vendor of F5 security appliances and evaluate the types of products and services they provide. Be prepared to explain to the class what appliances would be best to secure a midsized business.

Recommended Materials of Instruction

Ciampa, M. (2025). Security+ Guide to Network Security Fundamentals. *Cengage, 8th.* 9798214000633.
Whitman, M. E., & Mattord, H. J. (2022). Principles of Information Security. *Cengage, 7th.* 9780357506431.
CompTIA Certmaster Learn and Labs. *CompTIA, Security+ SYO-701.*

Minimum Qualifications

Computer Information Systems
Computer Science (Masters Required)
Computer Service Technology

Created/Revised by: Fischer, Linda
Date: 11/17/2025