# Lassen Community College Course Outline

## CIS 70 Computer and Network Security Fundamentals 3.0 Units

## I. Catalog Description

Introduces fundamental principles and topics of Information Technology Security and Risk Management at the organizational level. Addresses hardware, software, processes, communications, applications, and policies and procedures with respect to organizational Cybersecurity and Risk Management. Helps prepare for the CompTIA Security+ certification exams. This course has been approved for online delivery.

**Prerequisite(s):** Recommended CIS 50 IT Essentials

Does Not Transfer to UC/CSU
51 Hours Lecture, 102 Expected Outside Class Hours, 153 Total Student Learning Hours
Scheduled: Spring
CID ITIS 170

## II. Coding Information

Repeatability: Not Repeatable, Take 1 Time
Grading Graded
Credit Type: Credit
TOP Code: 0708.00
Scheduling: Every Spring

## III. Course Objectives

### A. Course Student Learning Outcomes

Upon completion of this course the student will be able to:

1. Analyze and implement security concepts and security policies.
2. Analyze common threats to and vulnerabilities of computer systems and networks.

### B. Course Objectives

Upon completion of this course, the student will 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.

## IV. Course Content

1. Introduction to Information Systems Security
2. Malware and Social Engineering Attacks
3. Application and Network Attacks
4. Vulnerability Assessment and Mitigating Attacks
5. Host, Application, and Data Security
6. Network Security
7. Administering a Secure Network
8. Wireless Network Security
9. Access Control Fundamentals
10. Authentication and Account Management
11. Basic Cryptography
12. Advanced Cryptography
13. Business Continuity
14. Risk Mitigation

## V. Assignments

**A. Reading Assignments**

1. Research the increasing threats to businesses.
2. Read the class text.

**B. Writing Assignments**

1. Create a security policy for a fictional business or entity.

**C. Quizzes**

1. Weekly online quizzes

**D. Virtual labs**

1. Labs relating to network monitoring, network scanning, wireless security, firewall implementation, digital certificates, RADIUS servers, and IPSec VPNs.

## VI. Methods of Evaluation

**Traditional Classroom Evaluation**

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

**Online Evaluation**

A. Exams/Tests
B. Quizzes

C. Virtual Lab Projects
D. Essays and research papers
E. Online Forum participation

## VII. Methods of Delivery

Check those delivery methods for which, this course has been separately approved by the Curriculum/Academic Standards Committee.

**X** Traditional Classroom Delivery ☐ Correspondence Delivery
☐ Hybrid Delivery **X** Online Delivery

**Traditional Classroom Delivery**
Lecture, discussion, group work, problem analysis, and interactive exercises

**Online Delivery**
Participation in forum based discussions. Online exercises/assignments contained on website. Web based video vignettes with discussion paper, email communications, postings to forums, online lecture notes and web links will compromise the method of instruction.

## VIII. Representative Texts and Supplies

**Cisco Network Academy Introduction to Cybersecurity v2.1** Netcad learning management system. (www.netacad.com) *Students will be provided with individual account access to the Cisco Netcad LMS. The complete curriculum for this course is available online for student use 24x7 through internet access and supports a range of computers for access*

**Cisco Network Academy Cybersecurity Essentials v2.1** Netcad learning management system. (www.netacad.com) *Students will be provided with individual account access to the Cisco Netcad LMS. The complete curriculum for this course is available online for student use 24x7 through internet access and supports a range of computers for access*

## IX. Discipline/s Assignment

Computer Information Systems

## X. Course Status

Current Status:
Original Approval Date: 11/16/2021
Board Approval Date: 12/14/2021
Revised By: Melinda Duerksen
Curriculum/Academic Standards Committee Revision Date: 03/21/2023