Course ID: CIMS 130
Cat ID: 433077.00
State ID: CCC000608645

College:	A	Saddleback College
Division/School:	BS	Business Science
Department:	CIM	Computer Information Management
Program:	CIMNAD	Network Administrator
Subject:	CIMNAD	Network Administrator

O F F I C I A L C O U R S E O U T L I N E

HISTORY AND STATUS

Course Status: A Active (Fully Approved)
Course Originator: Steve Korper

Board of Trustees	08/28/19
State Approval	04/20/05
Curriculum Committee Approval	07/24/19
Division Approval	07/24/19
Tech Review Approval	07/24/19

Technical Change Date: 03/05/01

Technical Change Comment:

3/5/01-taxonomy 2/25/13-fr CIM 284 to CIMS 230; 10/21/19 chng cb00 fr 404738 to 608645

Comments:

moe, assign, txt

BRIEF DESCRIPTION

Short Title: COMPTIA SECURITY+
Full Title: INTRO TO INFORMATION SYSTEMS SECURITY: COMPTIA SECURITY+

BRIEF DESCRIPTION

Catalog Description:

Provides a comprehensive overview of network security, information technology security and risk management at the organization level including authentication methods, common network attacks, safeguarding against attacks, remote access, email, the web, directory and file transfer, wireless data, various network devices and media, and proper use of perimeter topologies such as DMZs, Extranets, Intranets, basic and advance cryptography, and operational and organizational security. It addresses hardware, software, processes, communications, applications, and policies and procedures with respect to organizational Cybersecurity and Risk Management. Preparation for the CompTIA Security+ certificate. (Formerly CIMS 230).

Prerequisite:

None

Enrollment Limitation:

None

Corequisite:

None

Recommended Preparation:

None

COURSE FUNCTIONS

Course Prior to:	Y	Not Applicable
Course Classification:	Y	Credit Course
SC/IVC GE Code:	NA - Not Applicable	
CSU GE Code:	NA	Not Applicable
IGETC GE Code:	NA - Not Applicable	
UC Transferable Course:	N	No UC credit
Comparable SC/IVC:		
Comparable CSU:	CSU CSU Monterey Bay CST 282 - Introduction to Network Security	
Comparable UC:		
Comparable CCC Baccalaureate:		
TOP Code:	0708.10	Network Administrator
SAM Code:	D	Possibly Occupational
CAN Number:		
CID Number:		

COURSE OPTIONS

Grading Option:	GR	Letter Grade or Pass/No Pass
Open Entry:	N	No
Fixed, Optional or Variable Units:	F	Fixed Units
Repeatability Status:	N	No
Repeatability Model:		
Repeatability Limit:	0	
Cross-Listed Courses:	NONE	
Cross-Listed Parent:	No	

COURSE VALUES

Method of Instruction:	L-L	Lecture/Lab Combination	
Maximum Enrollment:	40	Maximum WSCH:	200
Average Enrollment:	22	Average WSCH:	110

	Lecture	Lab	Learn Ctr	Total
WFCH	2.00	3.00	0.00	5.00
TFCH	33.20	49.80	0.00	83.00
TSCH	33.20	49.80	0.00	83.00
LHE	2.00	2.50	0.00	4.50
FTEF	13.33	16.67	0.00	30.00
UNITS	2.00	1.00	0.00	3.00

Schedule Description:

Provides a comprehensive overview of network security, information technology security and risk management which is geared for students pursuing CompTIA Security+ Certification (formerly CIMS 230).

COURSE CONTENT
(Topics Covered)

Lecture Topics:

I. Introduction to Information System Security
II. Malware and Social Engineering Attacks
III. Application and Network Attacks
IV. Vulnerability Assessment and Mitigating Attacks
V. Host, Application and Data Security.
VI. Web and Network security
VII. Administering a Secure Network
VIII. Wireless, and instant messaging Network Security
IX. Access Control Fundamentals
X. Authentication and Account Management
XI. Basic Cryptography.
XII. Advanced Cryptography.
XIII. Disaster recovery and business continuity
XIV. Risk Mitigation.
XV. Network security topologies
XVI. Intrusion detection
XVII. Security Baselines

Lab/Learning Center Content:

I. Lab case examples covering malware and social engineering attacks
II. Lab case example covering vulnerability assessment and mitigating attacks
III. Lab case examples on wireless network security
IV. Lab case examples on basic and advanced cryptography
V. Labs on authentical and account management
VI. Labs on administering a secure network.

COURSE CONTENT
(Learning Objectives)

Students participating in this class will:

1. Introduction to Information Systems Security.
2. Explain social engineering, malware and social engineering attacks.
3. Application and network attacks.
4. List security ramifications, vulnerability assessment, mitigating attacks and costs of intrusion.
5. Host, application, and data security.
6. Network and specifically email security.
7. Administering a secure network.
8. Wireless network security.
9. Access control fundamentals.
10. Authentication and account management.
11. Apply concepts of using cryptography both basic and advanced.
12. Describe business continuity, risk mitigation and the disaster recovery planning process.
13. Analyze how intrusion detection systems operate.
14. Explain network hardening.
15. Describe the purpose of honeypots.

COURSE CONTENT
(Student Learning Outcomes)

Students completing this course satisfactorily will be able to:

1. Identify social engineering attacks, classify software attacks and identify hardware attacks
2. Define system components that are subject to attacks
3. Employ corporate security policy compliance, legal and physical security compliance and educate users with information

COURSE CONTENT
(Methods of Evaluation)

Evaluation of the student will be based upon the following items:

1. Writing Assignments
   short answers
   other (specify)
   a. Written examinations, which require the student to demonstrate knowledge of computer information security. b. Computer assignments requiring the student to demonstrate proficiency in the use of various security programs and intrusion detection systems.

2. Problem Solving Demonstrations
   quizzes
   other (specify)
   a. Computer assignments requiring the student to demonstrate proficiency in the use of various security programs and intrusion

detection systems.

3. Skill Demonstrations
   class performance(s)
   other (specify)
      a. Computer assignments requiring the student to demonstrate proficiency in the use of various security programs and intrusion detection systems.

4. Examinations
   multiple choice, true/false
   other (specify)
      a. Written examinations, which require the student to demonstrate knowledge of computer information security.

5. Other
   other (specify)
      a. Presentations relating to information security.

COURSE CONTENT
(In and Out-of-Class Assignments)

1. Typical Reading Assignments:
   Students will be expected to understand and critique college level technical documents or the equivalent. Reading assignments may include but are not limited to the following:

   a. Assigned Computer-Based courseware
   b. Technical papers
   c. Technical Web sites

2. Typical Writing Assignments:
   Writing assignments will pertain directly to the course topics and may include but are not limited to the following:

   a. Examinations and quizzes
   b. Lab exercises and problem simulations

3. Typical Oral Assignments:
   Class discussions

COURSE CONTENT
(Other Requirements)

Textbooks / Supplies:
Testout, TestOut Security Pro, Testout. 2016
Whitman, M. E. & Mattord, H. J., Principles of Information Security (MindTap Course List) , 6th Ed. Cengage Learning. 2017
Ciampa, M., CompTIA Security+ Guide to Network Security Fundamentals, 6th Ed. Cengage Learning. 2017

Material Fees: $ 0.00 Transaction Code:

VALIDATION
(Corequisite, Limitation on Enrollment,
Prerequisite and Recommended Preparation)