CS 82.58 Course Outline as of Fall 2021

CATALOG INFORMATION

Dept and Nbr: CS 82.58 Title: INTRO CYBERSEC
Full Title: Introduction to Information Systems Security
Last Reviewed: 2/22/2021

Units		Course Hours per Week		Nbr of Weeks	Course Hours Total	
Maximum	3.00	Lecture Scheduled	3.00	17.5	Lecture Scheduled	52.50
Minimum	3.00	Lab Scheduled	0	8	Lab Scheduled	0
		Contact DHR	0		Contact DHR	0
		Contact Total	3.00		Contact Total	52.50
		Non-contact DHR	0		Non-contact DHR	0

Total Out of Class Hours: 105.00 Total Student Learning Hours: 157.50

Title 5 Category:	AA Degree Applicable
Grading:	Grade or P/NP
Repeatability:	00 - Two Repeats if Grade was D, F, NC, or NP
Also Listed As:	
Formerly:	

Catalog Description:
An introduction to the fundamental principles and topics of Information Technology Security and Risk Management at the organizational level. It provides in-depth coverage of the current risks and threats to an organization’s data, combined with a structured way of addressing the safeguarding of these critical electronic assets. Additionally, the course provides the broad-based knowledge necessary to prepare students for further study in other specialized security fields. It is also intended to serve the needs of individuals seeking to pass the Computing Technology Industry Association’s (CompTIA) Security+ certification exam.

Prerequisites/Corequisites:

Recommended Preparation:
Eligibility for ENGL 100 or ESL 100 or appropriate placement based on AB705 mandates; and Completion of CS 82.22A

Limits on Enrollment:

Schedule of Classes Information:
Description: An introduction to the fundamental principles and topics of Information

Technology Security and Risk Management at the organizational level. It provides in-depth coverage of the current risks and threats to an organization's data, combined with a structured way of addressing the safeguarding of these critical electronic assets. Additionally, the course provides the broad-based knowledge necessary to prepare students for further study in other specialized security fields. It is also intended to serve the needs of individuals seeking to pass the Computing Technology Industry Association's (CompTIA) Security+ certification exam. (Grade or P/NP)
Prerequisites/Corequisites:
Recommended: Eligibility for ENGL 100 or ESL 100 or appropriate placement based on AB705 mandates; and Completion of CS 82.22A
Limits on Enrollment:
Transfer Credit: CSU;
Repeatability: Two Repeats if Grade was D, F, NC, or NP

ARTICULATION, MAJOR, and CERTIFICATION INFORMATION:

AS Degree:	**Area**			Effective:	Inactive:
CSU GE:	**Transfer Area**			Effective:	Inactive:
IGETC:	**Transfer Area**			Effective:	Inactive:
CSU Transfer:	Transferable	Effective:	Fall 2021	Inactive:	
UC Transfer:		Effective:		Inactive:	

CID:

Certificate/Major Applicable:
Not Certificate/Major Applicable

COURSE CONTENT

Student Learning Outcomes:
At the conclusion of this course, the student should be able to:
1. Demonstrate methods to protect computer systems against security vulnerabilities
2. Develop a Business Disaster Recovery Plan

Objectives:
Students will be able to:

1. Describe why information security is essential in today's IT environment
2. Identify the goals of information security
3. Describe common security threats and their ramifications
4. Determine the factors involved in developing a secure information security strategy
5. Identify common attacks and describe how to safeguard against them
6. Describe communications, E-mail, Web, remote access, and wireless security issues
7. Evaluate various network devices and media and how best to secure them
8. Describe the basics of cryptography
9. Differentiate between physical security, disaster recovery, and business continuity
10. Utilize network diagrams to implement wireless network security, access controls, and risk mitigation

11. Demonstrate appropriate and ethical behavior and good work habits

Topics and Scope:

1. Introduction to Information Systems Security, Ethical Behavior, and Good Work Habits
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

Assignment:

Reading assignments include:
1. Online research of security devices and deployment practices
2. Approximately 50 pages weekly from the textbook

Homework problems include:
1. Weekly online discussion thread participation
2. Hands-on exercises and class performances to demonstrate proficiency with topics
3. Online quizzes
4. Homework assignments may include assignments securing various system environments

Other assignments include:
1. Quizzes (9 -11) and skill demonstration exam
2. Classroom scenario-based exercises

Methods of Evaluation/Basis of Grade:

Writing: Assessment tools that demonstrate writing skills and/or require students to select, organize and explain ideas in writing.

Weekly written online discussions	Writing 5 - 10%

Problem Solving: Assessment tools, other than exams, that demonstrate competence in computational or non-computational problem solving skills.

Homework problems, assignments securing various system environments	Problem solving 15 - 30%

Skill Demonstrations: All skill-based and physical demonstrations used for assessment purposes including skill performance exams.

Skill demonstration exam	Skill Demonstrations 20 - 30%

Exams: All forms of formal testing, other than skill performance exams.

Quizzes and skill demonstration exam	Exams 20 - 30%

Other: Includes any assessment tools that do not logically fit into the above categories.

Attendance and participation in scenario-based exercises	Other Category 5 - 20%

Representative Textbooks and Materials:
CompTIA Security+ Study Guide: Exam SY0-601. 8th ed. Chapple, Mike and Seidl, David. Wiley. 2021
CompTIA Security+ Guide to Network Security Fundamentals. 6th ed. Ciampa, Dr. Mark. Cengage Learning. 2017
CompTIA Security+ Certification All-in-One Exam Guide: Exam SY0-601. 6th ed. Conklin, William. Arthur. McGraw-Hill Education. 2021