هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

T-104
2022

Course Specification

Course Title:	Information Security
Course Code:	279 CIS-3
Program:	Applied Information Systems
Department:	Computer
College:	Applied College
Institution:	Najran University
Version:	**T-104 2022**
Last Revision Date:	**20/8/2023**

Table of Contents:

A. General information about the course:

Course Identification					
1. Credit hours:	3 (2+2)				
2. Course type					
a.	University ☐	College ☐	Department☒	Track☐	Others☐
b.	Required ☒	Elective☐			
3. Level/year at which this course is offered: ***Level 4***					
4. Course general Description					
5. Pre-requirements for this course (if any): 168 CIS-3					
6. Co- requirements for this course (if any):					

7. Course Main Objective(s)

• Understand and contextualize the principles of information security in complex systems and organizations
• Understand, implement, and develop cyber security controls, security policies, procedures, and programs
• Perform threat, vulnerability, and risk assessments
• Plan a security awareness, training, and education activity

1. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1.	Traditional classroom	56	95%
2.	E-learning		5%
3.	Hybrid • Traditional classroom • E-learning		
4.	Distance learning		

2. Contact Hours (based on the academic semester)

No	Activity	Contact Hours
1.	Lectures	28 Hours
2.	Laboratory/Studio	28 Hours
3.	Field	-
4.	Tutorial	-
5.	Others (specify)	
	Total	56 Hours

B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
1.0	Knowledge and understanding			
1.1	List and discuss the key characteristics of information security	K1=p	• Lectures, labs • Brainstorming, • Class Discussion	• Class work • assignments • Quizzes • Midterm • Exams • Final Exam
1.2	understand information security policy role in a successful information security program	K2=I	• Lectures, labs • Brainstorming, • Class Discussion	• Class work • assignments • Quizzes • Midterm • Exams • Final Exam
…				
2.0	Skills			
2.1	analysis the principal components of information security (InfoSec) system implementation planning in the organizational planning scheme	S3=I	• Class • Discussion • Related • Computer Software and websites	• • Class work • assignments • Quizzes • Midterm • Exams • Final Exam

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
2.2	Discuss the need for contingency planning			
2.3	Explain the organizational approaches to information security			
3.0	Values, autonomy, and responsibility			
3.1	The student is committed to work ethics in the work environment	V1=I	• Brainstorming, • Class Discussion	• Assignment • Class work
3.2				

C. Course Content

No	List of Topics	Contact Hours
1.	Course Overview and Logistics Information Security Environment Lab:X	2 2
2.	INTRODUCTION TO INFORMATION SECURITY Lab:X	2 2
3	PLANNING FOR SECURITY Lab : Performing Reconnaissance and Probing using Common Tools	4 4
4	PLANNING FOR CONTINGENCIES Lab:Performing a Vulnerability Assessment	2 2
5	INFORMATION SECURITY POLICY (Security Education, Training and Awareness) Lab: Performing a Web Site and Database Attack by Exploiting Identified Vulnerabilities	2 2
6	**Mid Exam**	2

7	DEVELOPING THE SECURITY PROGRAM Lab: Implementing an Information Systems Security Policy	2 2
8	SECURITY MANAGEMENT MODELS Lab :Implementing an Information Systems Security Policy	2 2
9	SECURITY MANAGEMENT PRACTICES Lab: Implementing an Information Systems Security Policy	2 2
10	PERSONNEL AND SECURITY Lab: Implementing a Business Continuity Plan	2 2
11	RISK MANAGEMENT: IDENTIFYING AND ASSESSING RISK Lab :Enabling Windows Active Directory and User Management: A Modern Fairy Tale" Access Control	2 2
12	RISK MANAGEMENT: CONTROLLING RISK Lab: Enabling Windows Active Directory and User Management: A Modern Fairy Tale" Access Control	2 2
13	Economics of Cyber security: Economic Aspects of Information Security	2
14	LAW AND ETHICS	2
15	**Practice exam**	2
Total		**56**

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	assignment	2-13	10%
2.	Mid exam	8	20%
3.	Practical exam	14	20%
...	Final exam	End of the semster	50%

*Assessment Activities (i.e., Written test, oral test, oral presentation, group project, essay, etc.)

E. Learning Resources and Facilities

1. References and Learning Resources

Essential References	Michael E. Whitman, Herbert J. Mattord, Management of Information Security, Latest Edition. Course Technology, Cengage Learning, ISBN-13: 978-1-285-06229-7.
Supportive References	*Computer Security: Art and Science*, Matt Bishop (ISBN: 0-201-44099-7), Addison-Wesley 2003 *Security Engineering: A Guide to Building Dependable Distributed Systems*, Ross Anderson, Wiley, John & Sons, Incorporated, 2001
Electronic Materials	
Other Learning Materials	*Guide to Disaster Recovery*, M. *Erbschilde*

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	Lecture rooms should be large enough to accommodate the number of registered students
Technology equipment (projector, smart board, software)	Data Show
Other equipment (depending on the nature of the specialty)	Wireshark software

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Students	End term Questionnaire
Effectiveness of students assessment	Head of the department and Departmental Council discussions	Directly
Quality of learning resources		
The extent to which CLOs have been achieved		
Other		

Assessor (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)

Assessment Methods (Direct, Indirect)

G. Specification Approval Data

COUNCIL /COMMITTEE	
REFERENCE NO.	
DATE