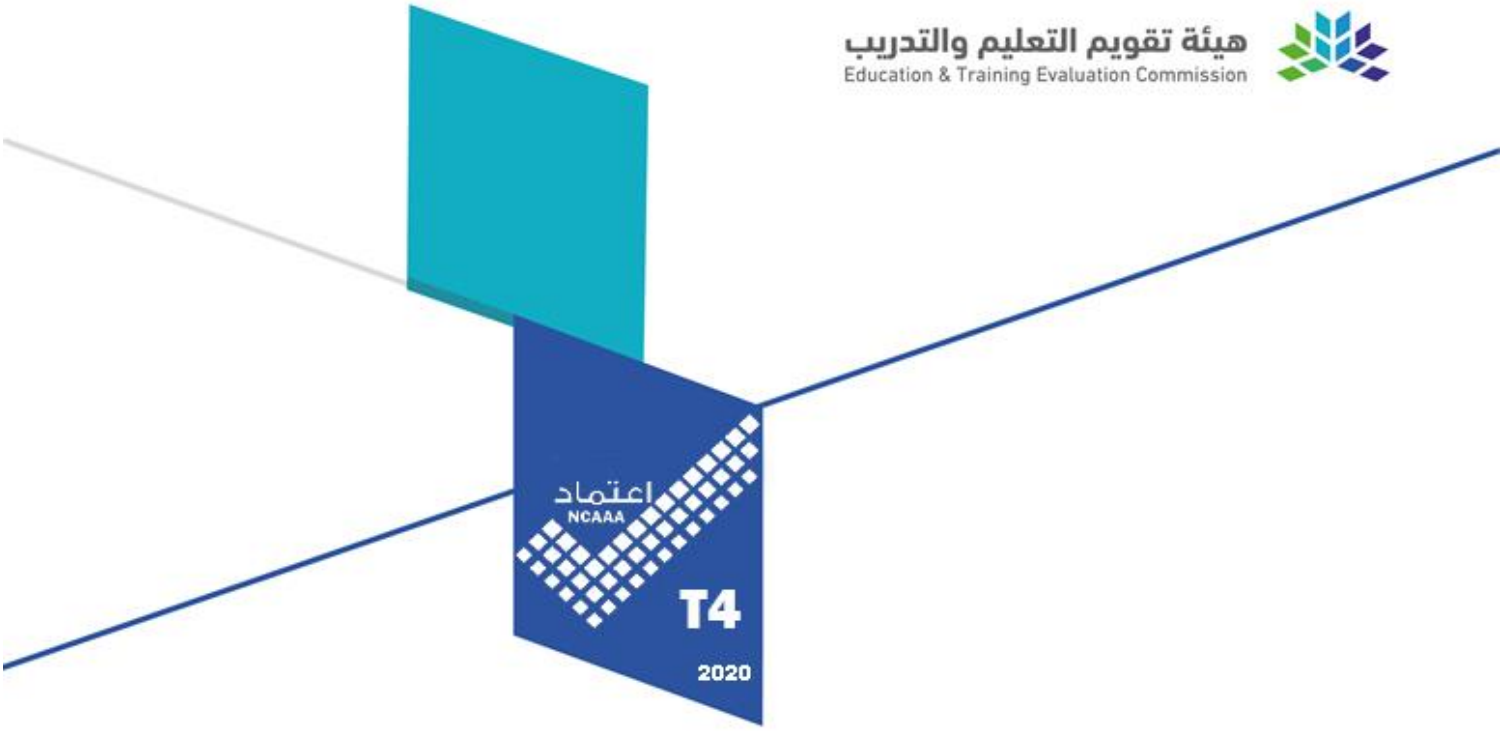
هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission



Course Specifications

Course Title:	Information Security
Course Code:	**CSI 447**
Program:	**Computer Science and Information Technology**
Department:	**Computer Science and Information**
College:	**Science**
Institution:	**Majmaah University**

Table of Contents

A. Course Identification

1. Credit hours:	3 (2 lecture + 2 lab)
2. Course type	
a.	University ☐ College ☐ Department ☑ Others ☐
b.	Required ☐ Elective ☑
3. Level/year at which this course is offered:	**From level 7 year 4**
4. Pre-requisites for this course (if any)**:**	Cryptography and Information Security (CSI 423)
5. Co-requisites for this course (if any)**:**	**Nan**

6. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	**Traditional classroom**	48	80%
2	**Blended**	6	10%
3	**E-learning**	6	10%
4	**Distance learning**	0	0%
5	**Other**	0	0%

7. Contact Hours (based on academic semester)

No	Activity	Contact Hours
1	**Lecture**	30
2	**Laboratory/Studio**	30
3	**Tutorial**	0
4	**Others** (specify)	0
	Total	60

B. Course Objectives and Learning Outcomes

1. Course Description

This course is to make students familiar with the basic concepts of information systems security. The course aims to the security goals, security functions, and security mechanisms. The content is: Introduction to information security, information security and risk management, access control, security architecture and design, physical environmental security, telecommunications and network security, business continuity and disaster recovery, application security and operation security. The choice of appropriate encryption/decryption is the key in the development of efficient secure information system. In fact, it is difficult to create a trusted information system without a good understanding of a number of fundamental information security issues.

2. Course Main Objective

This course aims:

1. To learn how the choice of encryption and decryption algorithm design methods impacts the performance of any information system.
2. To learn how to define the security problems.
3. To study specific algorithms for encryption and decryption.
4. To study a wide spectrum of different issues where we can protect our information systems

3. Course Learning Outcomes

CLOs		Aligned PLOs
1	**Knowledge and Understanding**	
1.1	Explain the objectives of information security.	
1.2	Discuss the importance and applications of each of confidentiality, integrity, and availability.	
1.3	Understand the basic categories of threats to computers and networks.	
2	**Skills :**	
2.1	Analyze issues for creating security policy for a large organization.	
2.2	Defend the need for protection and security, and the role of ethical considerations in computer use.	
2.3	Present issues and solutions in appropriate form to communicate effectively with peers and clients from specialist and non-specialist backgrounds.	
3	**Values:**	
3.1	Analyze the local and global impact of information security on individuals, organizations, and society	
3.2	Function effectively on teams to accomplish a common goal.	

C. Course Content

No	List of Topics	Contact Hours
1	Introduction to information Security: History of information security, what is security? CNSS Security Model, Security systems development life cycles, security professionals and organization, the need for security, business needs first, threats, attacks, secure software developments, legal, ethical and professional issues in information security.	12
2	Information security and risk management: an overview of risk management, risk identification, risk assessment, risk control strategies, selecting a risk control strategy.	16
3	Security technology: access control, Firewalls, protecting remote connections, intrusion detection and prevention systems.	16
4	Physical environmental security: physical access control, fire security and safety, failure of supporting utilities, mobile and portable systems.	16
Total		60

D. Teaching and Assessment

1. Alignment of Course Learning Outcomes with Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
1.0	**Knowledge and Understanding**		
1.1	Explain the objectives of information security.	Lectures Lab demonstrations Case studies Individual presentations	Written Exam Homework assignments Lab assignments Class Activities Quizzes
1.2	Discuss the importance and applications of each of confidentiality, integrity, and availability.		
1.3	Understand the basic categories of threats to computers and networks.		
2.0	**Skills**		
2.1	Analyze issues for creating security policy for a large organization.	Lectures Lab demonstrations Case studies Individual presentations Brainstorming	Written Exam Homework assignments Lab assignments Class Activities Quizzes Observations
2.2	Defend the need for protection and security, and the role of ethical considerations in computer use.		
2.3	Present issues and solutions in appropriate form to communicate effectively with peers and clients from specialist and non-specialist backgrounds.		
3.0	**Values**		
3.1	Analyze the local and global impact of information security on individuals, organizations, and society	Small group discussion Whole group discussion Brainstorming Presentation	Observations Homework assignments Lab assignments Class Activities
3.2	Function effectively on teams to accomplish a common goal.		

2. Assessment Tasks for Students

#	Assessment task*	Week Due	Percentage of Total Assessment Score
1	First written mid-term exam	6	15%
2	Second written mid-term exam	12	15%
3	Presentation, class activities, and group discussion	Every week	10%
4	Homework assignments	After each chapter	10%
5	Implementation of presented algorithms	Every two weeks	10%
6	Final written exam	16	40%
7	T Total		100%

***Assessment task** (i.e., written test, oral test, oral presentation, group project, essay, etc.)

E. Student Academic Counseling and Support

Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice :
Office hours: Sun: 10-12, Mon. 10-12, Thru 8-10 Office call: Sun. 12-1 and Wed 12-1 Email: h.haly@mu.edu.sa Mobile: 0538231332

F. Learning Resources and Facilities

1.Learning Resources

Required Textbooks	Michael E. Whitman, Herbert J. Mattord, Principles of information security, Cengage Learning, 2013.
Essential References Materials	W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, Six Edition. 2013.
Electronic Materials	www.iacr.org
Other Learning Materials	NaN

2. Facilities Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	Classroom and Labe available at College of science in Zulfi.
Technology Resources (AV, data show, Smart Board, software, etc.)	All resource are available in the halls
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	N\A

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Effectiveness of teaching and assessment	Students Reviewers	Questionnaires (course evaluation) filled by the students and electronically organized by the university. Student-faculty and management meetings.

Evaluation areas (e.g., Effectiveness of teaching and assessment, Extent of achievement of course learning outcomes, Quality of learning resources, etc.)
Evaluators (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)
Assessment Methods (Direct, Indirect)

H. Specification Approval Data

Council / Committee		د عبد الله إبراهيم العريني
Reference No.		رئيس قسم علوم الحاسب والمعلومات
Date		28.04.2021