Course Specifications

Course Title:	**Network Security**
Course Code:	**CSI-432**
Program:	**Computer Science and Information Technologies**
Department:	**Computer Science and Information**
College:	**College of Science at Az Zulfi**
Institution:	**Majmaah University**

Table of Contents

A. Course Identification

1. Credit hours:	
2. Course type	
a. University ☐ College ☐ Department ☒ Others ☐	
b. Required ☐ Elective ☐	
3. Level/year at which this course is offered: **Elective**	
4. Pre-requisites for this course (if any)**:** **Advanced Computer Networks (CSI 431)**	
5. Co-requisites for this course (if any)**:** **N/A**	

6. Mode of Instruction (mark all that apply)

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

7. Actual Learning Hours (based on academic semester)

No	Activity	Learning Hours
Contact Hours		
1	**Lecture**	30
2	**Laboratory/Studio**	30
3	**Tutorial**	-
4	**Others** (specify)	-
	Total	60
Other Learning Hours*		
1	**Study**	-
2	**Assignments**	-
3	**Library**	-
4	**Projects/Research Essays/Theses**	5
5	**Others** (specify)	-
	Total	5

* The length of time that a learner takes to complete learning activities that lead to achievement of course learning outcomes, such as study time, homework assignments, projects, preparing presentations, library times

B. Course Objectives and Learning Outcomes

1. Course Description

This course provides an introduction to the field of network security. Specific topics to be examined include security attacks, mechanisms, and services, network security, access security models, network security practice, Email security, IP security , web security, Intrusion detection , prevention systems , firewalls and virtual private networks , cellular and wireless network security.

2. Course Main Objective

This module aims :
1. To introduce students with the importance of security for computer systems.
2. To describe the security goals and the services of security system.
3. To explain available methods of defense.
4. To distinguish among Transport-Levels Security such as, Web Security Issues, Secure Sockets Layer (SSL) and Transport Layer Security (TLS).
5. To understand Wireless Network Security and explains the general idea of, IEEE 802.11 Wireless LAN Overview, IEEE 802.11i Wireless LAN Security, Wireless Application, Protocol Overview, Wireless Transport Layer Security and WAP End-to-End Security.

3. Course Learning Outcomes

	CLOs		Aligned PLOs
1	**Knowledge:**		
1.1	Demonstrate knowledge and understanding of essential facts, concepts, theories and principles of secure networking systems, and its underpinning science and mathematics;		K1
1.2	Asses the threats, vulnerabilities, and risks to a computer network.		K2
1.3	Identify the standards of security protocols for Emails, web security, and IP security.		K3
2	**Skills :**		
2.1	Demonstrate creative and innovative ability in the synthesis of solutions and in formulating designs in secure computer network systems;		S1
2.2	Apply relevant analytical and modeling techniques for specification and design of security based systems.		S2
3	**Competence:**		
3.1	Work in a group and learn time management		C1
3.2	Learn how to search for information through library and internet.		C2
3.3	Present a short report in a written form and orally using appropriate scientific language		C3

C. Course Content

No	List of Topics	Contact Hours
1	Introduction	4

	.The importance of network security	
2	**Key Distribution and User Authentication** • Symmetric Key Distribution Using Symmetric Encryption • Kerberos • Key Distribution Using Asymmetric Encryption • X.509 Certificates • Public Key Infrastructure • Federated Identity Management	12
3	**Transport-Level Security** • Web Security Issues • Secure Sockets Layer (SSL) • Transport Layer Security (TLS) • HTTPS • Secure Shell (SSH)	12
4	**Wireless Network Security** • IEEE 802.11 Wireless LAN Overview • IEEE 802.11i Wireless LAN Security • Wireless Application Protocol Overview • Wireless Transport Layer Security • WAP End-to-End Security	12
5	**IP Security** • IP Security Overview • IP Security Policy • Encapsulating Security Payload • Combining Security Associations • Internet Key Exchange • Cryptographic Suites	12
6	**Email Security** • PGP • S/MIME • Domain Keys Identifications Mail	8
Total		

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**		

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
1.1	Demonstrate knowledge and understanding of essential facts, concepts, theories and principles of secure networking systems, and its underpinning science and mathematics;	Lectures. Lab demonstrations. Case studies. Individual presentations	Written Exam Homework assignments Lab assignments Class Activities Quizzes
1.2	Asses the threats, vulnerabilities, and risks to a computer network.		
1.3	Identify the standards of security protocols for Emails, web security, and IP security.		
2.0	**Skills**		
2.1	Demonstrate creative and innovative ability in the synthesis of solutions and in formulating designs in secure computer network systems;	Lectures. Lab demonstrations. Case studies. Individual presentations. Brainstorming.	Written Exam Homework assignments Lab assignments Class Activities Quizzes Observations
2.2	Apply relevant analytical and modeling techniques for specification and design of security based systems.		
3.0	**Competence**		
3.1	Set up, test and administer security systems for effective use;	Small group discussions. Whole group discussions. Brainstorming. Presentations.	Observations Homework assignments Lab assignments Class Activities
3.2	Make effective oral presentations, both formally and informally		

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 protocols	Every two weeks	10%
6	Final written exam	16	40%
7	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 :

1. A total of 6 office hours per week in the lecturer schedule in order to facilitate the student.
2. Contacting students using e-mail , mobile, office telephone and website

F. Learning Resources and Facilities

1.Learning Resources

Required Textbooks	Czarnul, P. (2018). Parallel Programming for Modern High Performance Computing Systems. Chapman and Hall/CRC.
Essential References Materials	• Douglas Jacobson, Introduction to Network Security, Taylor & Francis, 2008. • W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, Six Edition. 2013.
Electronic Materials	www.iacr.org
Other Learning Materials	**N/A**

2. Facilities Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	Classrooms and Labs as that available at college of science at Az-Zulfi are enough.
Technology Resources (AV, data show, Smart Board, software, etc.)	Smart Board
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	Students	• Analysis of students' results. Observation during class work. • Students' evaluations. • Colleagues' evaluations. • Evaluation questionnaire filled by the students.

Evaluation Areas/Issues	Evaluators	Evaluation Methods
		Interview a sample of students enrolled in the course to take their opinions
Evaluation of Teaching	Program leaders	• Self-assessment. • External evaluation. Periodic review of course (the Commission of study plans)

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	
Reference No.	
Date	