Course Specifications

Course Title:	**Cyber Security Essentials**
Course Code:	**CSEC 323**
Program:	**Information and Computer Science**
Department:	**Computer Science and Information**
College:	**Science at AL-Zulfi**
Institution:	**Majmaah University**

Table of Contents

A. Course Identification

1. Credit hours: **3**
2. Course type **a.** University ☐ College ☐ Department ☐ Others ☑ **b.** Required ☑ Elective ☐
3. Level/year at which this course is offered: Level six , 6th semester
4. Pre-requisites for this course (if any)**:** CSEC 313
5. Co-requisites for this course (if any)**: Nil**

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**	60
2	**Laboratory/Studio**	45
3	**Tutorial**	
4	**Others** (specify)	
	Total	
Other Learning Hours*		
1	**Study**	
2	**Assignments**	
3	**Library**	
4	**Projects/Research Essays/Theses**	
5	**Others** (specify)	
	Total	

* 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

Introduction to data integrity and authentication, authentication strength (Multifactor authentication, Cryptographic tokens, Cryptographic devices etc.), Password attack techniques (Dictionary attack, Brute force attack, Malware-based attack, Off-line analysis, and Password cracking tools), Password storage techniques (Cryptographic hash functions - SHA-256, SHA-3, collision resistance, Salting, Password-based key derivation), Data integrity (Message authentication codes such as HMAC, CBC-MAC, Digital signatures, Authenticated encryption, and Hash trees), Authentication of evidence (Hashing algorithms such asMD5, SHA-1), Secure Communication Protocols (Application and transport layer protocols such as HTTP, HTTPS, SSH, and SSL/TLS, Attacks on TLS-Downgrade attacks, Certificate forgery, Implications of stolen root certificates, and Certificate transparency, Privacy preserving protocols such as Mixnet, Tor, Off-the-record message, and Signal), Cryptanalysis Classical attacks (Brute-force attack,Side-channel attacks, Attacks against privatekey ciphers, Attacks against publickey ciphers, Attacks on RSA).

2. Course Main Objective

1. Provide students with an understanding of the basics of data security.
2. Provide students with an understanding of the fundamental design principles of software security.
3. Provide students with an understanding of the essentials of component security.
4. Provide students with an understanding of the essentials of system security.
5. Provide students with an understanding of the basics of data security.

3. Course Learning Outcomes

CLOs		Aligned PLOs
1	**Knowledge:**	
1.1	Differentiate the various types of security from a computer systems perspective (e.g. Cybersecurity, email security, physical security, etc.).	K1
1.2	Describe various basic security practices (e.g. strong passwords, firewalls, account controls, file privacy, etc.)	K1
1.3	Describe and demonstrate appropriate file backup techniques	K1
1.4	Describe basic computer log entries and identify potential security issues	K3-CS
1.5	Identify several techniques appropriate to provide basic protection of a small computer and/or small network	K3-CS
1.6	Describe basic incident response techniques	K3-CS
2	**Skills :**	
2.1	Create a user account on a computer using basic security techniques	S1
2.2		
2.3		
2...		
3	**Competence:**	
3.1	Work cooperatively in a small group environment.	C2
3.2		
3.3		
3...		

C. Course Content

No	List of Topics	Contact Hours
1	Essentials of cyber security: Basic cryptography concepts, - Digital forensics, - End-to-end secure communications, - Data integrity and authentication, and - Information storage security.	8
2	Attackers techniques and motivations: Fundamental design principles including least privilege, open design, and abstraction, - Security requirements and their role in design, - Implementation issues, - Static and dynamic testing, - Configuring and patching, and - Ethics, especially in development, testing and vulnerability disclosure.	8
3	Exploitation: Vulnerabilities of system components, - Component lifecycle, - Secure component design principles, - Supply chain management security, - Security testing, and - Reverse engineering.	12
4	Essentials of Connection Security: Systems, architecture, models, and standards, - Physical component interfaces, - Software component interfaces, - Connection attacks, and - Transmission attacks.	12
5	Defense and analysis techniques: Holistic approach, - Security policy, - Authentication, - Access control, - Monitoring, - Recovery, - Testing, and - Documentation.	12
6	Essentials of Human Security: Identity management, - Social engineering, - Awareness and understanding, - Social behavioral privacy and security, and - Personal data privacy and security.	12
Total		64

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**		
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	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	Written Exam Homework assignments

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
2.2	Apply relevant analytical and modeling techniques for specification and design of security based systems	Case studies Individual presentations Brainstorming	Lab assignments Class Activities Quizzes
…			
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	Develop and implement a security plan as it relates to the network components of an organization		
…			

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	11	15%
3	Homework assignments	Every week	10%
4	Presentation, class activities, and group discussion	After Every chapter	10%
5	E – Quiz	12	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 :

F. Learning Resources and Facilities

1.Learning Resources

Required Textbooks	J. Graham, R. Howard, R. Olson "Cyber security essentials", CRC Press 2016
Essential References Materials	J. Pande" Introduction to Cyber Security", Uttarakhand Open University 2017
Electronic Materials	Video lectures

Other Learning Materials	

2. Facilities Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	Classrooms and Laboratories, as those that are available at the college of science at AzZulfi.
Technology Resources (AV, Classrooms and Laboratories, as those that are available at the college of science at AzZulfi., etc.)	Classrooms and Laboratories, as those that are available at the college of science at AzZulfi.
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	None

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Effectiveness of teaching and assessment.	Program Leaders	Direct
Quality of learning resources	Faculty	Indirect
Extent of achievement of course learning outcomes	Peer Reviewer	Direct
	Students'	
	Colleagues	
	Self-assessment	

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	