



# Course Specification

## (Bachelor)

Course Title: **Cybersecurity Design Principles**

Course Code: **APIS2206**

Program: **Information Security Diploma**

Department: **Diplomas**

College: **Applied College**

Institution: **Umm Al-Qura university**

Version: **1.0**

Last Revision Date: **13 December 2024**



## Table of Contents

A. General information about the course: .....	3
B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods .....	4
C. Course Content.....	5
D. Students Assessment Activities .....	6
E. Learning Resources and Facilities.....	6
F. Assessment of Course Quality .....	7
G. Specification Approval .....	7





## A. General information about the course:

### 1. Course Identification

1. Credit hours: ( 2 )

#### 2. Course type

A. ☐ University ☐ College ☒ Department ☐ Track ☐ Others  
B. ☒ Required ☐ Elective

3. Level/year at which this course is offered: ( Level 2, 1<sup>st</sup> year )

#### 4. Course General Description:

This course includes the knowledge and skills of the fundamentals of secure-by-design for designing secure and reliable cyber systems.

#### 5. Pre-requirements for this course (if any):

Introduction to Cybersecurity

#### 6. Co-requisites for this course (if any):

None

#### 7. Course Main Objective(s):

The intent of this course is to provide students with basic security design fundamentals that help create systems that are worthy of being trusted.

### 2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	30	100%
2	E-learning		
3	Hybrid <ul style="list-style-type: none"> <li>Traditional classroom</li> <li>E-learning</li> </ul>		
4	Distance learning		



### 3. Contact Hours (based on the academic semester)

No	Activity	Contact Hours
1.	Lectures	30
2.	Laboratory/Studio	
3.	Field	
4.	Tutorial	
5.	Others (specify)	
Total		30

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

Code	Course Learning Outcomes	Code of PLOs aligned with the program	Teaching Strategies	Assessment Methods
1.0	Knowledge and understanding			
1.1	Express the secure-by-design principles.	K1	Lecture	Assignments, Quizzes, Exams
1.2	Explain the importance of cybersecurity design principles and how each principle is useful to design trusted systems.	K2	Lecture	Assignments, Quizzes, Exams
2.0	Skills			
2.1	Distinguish the violated design principle for common system security weaknesses.	S1	Lecture	Assignments, Quizzes, Exams
2.2	Analyze the required cybersecurity design principles needed for a given setup.	S1	Lecture	Assignments, Quizzes, Exams
2.4	Apply cybersecurity design principles to complex programs and / or systems.	S4	Lecture	Assignments, Quizzes, Exams





Code	Course Learning Outcomes	Code of PLOs aligned with the program	Teaching Strategies	Assessment Methods
3.0	Values, autonomy, and responsibility			
3.1	Be an independent learner, able to acquire further knowledge with some guidance or support.	V2	Lecture	Assignments, Quizzes, Exams

### C. Course Content

No	List of Topics	Contact Hours
1.	Fundamentals and Importance of the Secure Design for Programs and Systems	2
2.	Important principles in secure system design	2
3.	Separation of Duties, Encapsulation	2
4.	Modularity, Simplicity of Design	2
5.	Minimization of Implementation	2
6.	Open Design	2
7.	Complete Mediation	2
8.	Layering and Defense-in-Depth	2
9.	Models of Systems Security Levels and Access Privileges	2
10.	Fail Safe Defaults and Fail Secure	2
11.	Least Astonishment	2
12.	Minimize Trust Surface	2
13.	Secure Design and Usability	2
14.	Trust Relationships	2
15.	Secure Coding Patterns	2
Total		30





## D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Assignment	Throughout Semester	15%
2.	Quizzes	Throughout Semester	20%
3.	Midterm Exam	8	25%
4.	Final Exam	Finals Week	40%

\*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	Merkow, M. S. (2022). Practical Security for Agile and DevOps. CRC Press.
Supportive References	<ul style="list-style-type: none"> <li>Benzel, T. V., Irvine, C. E., Levin, T. E., Nguyen, T. D., Clark, P. C., &amp; Bhaskare, G. (2005). <i>Design principles for security</i>. Monterey, California. Naval Postgraduate School</li> <li>"Security Engineering: A Guide to Building Dependable Distributed Systems" by Ross Anderson, Third edition, 2020</li> </ul>
Electronic Materials	
Other Learning Materials	

### 2. Required Facilities and equipment

Items	Resources
<b>facilities</b> (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	<b>Traditional Classroom</b>
<b>Technology equipment</b> (projector, smart board, software)	<b>Multimedia Projector</b>
<b>Other equipment</b> (depending on the nature of the specialty)	



## F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Students	Survey at the end of the course
Effectiveness of Students assessment	Instructor	Course Report
Quality of learning resources	Instructor	Survey at the end of the course
The extent to which CLOs have been achieved	Instructor	Course Report
Other		

**Assessors** (Students, Faculty, Program Leaders, Peer Reviewers, Others (specify))

**Assessment Methods** (Direct, Indirect)

## G. Specification Approval

<b>COUNCIL /COMMITTEE</b>	Umm Al-Qura University Council
<b>REFERENCE NO.</b>	851141114462/190358
<b>DATE</b>	1446/11/22

