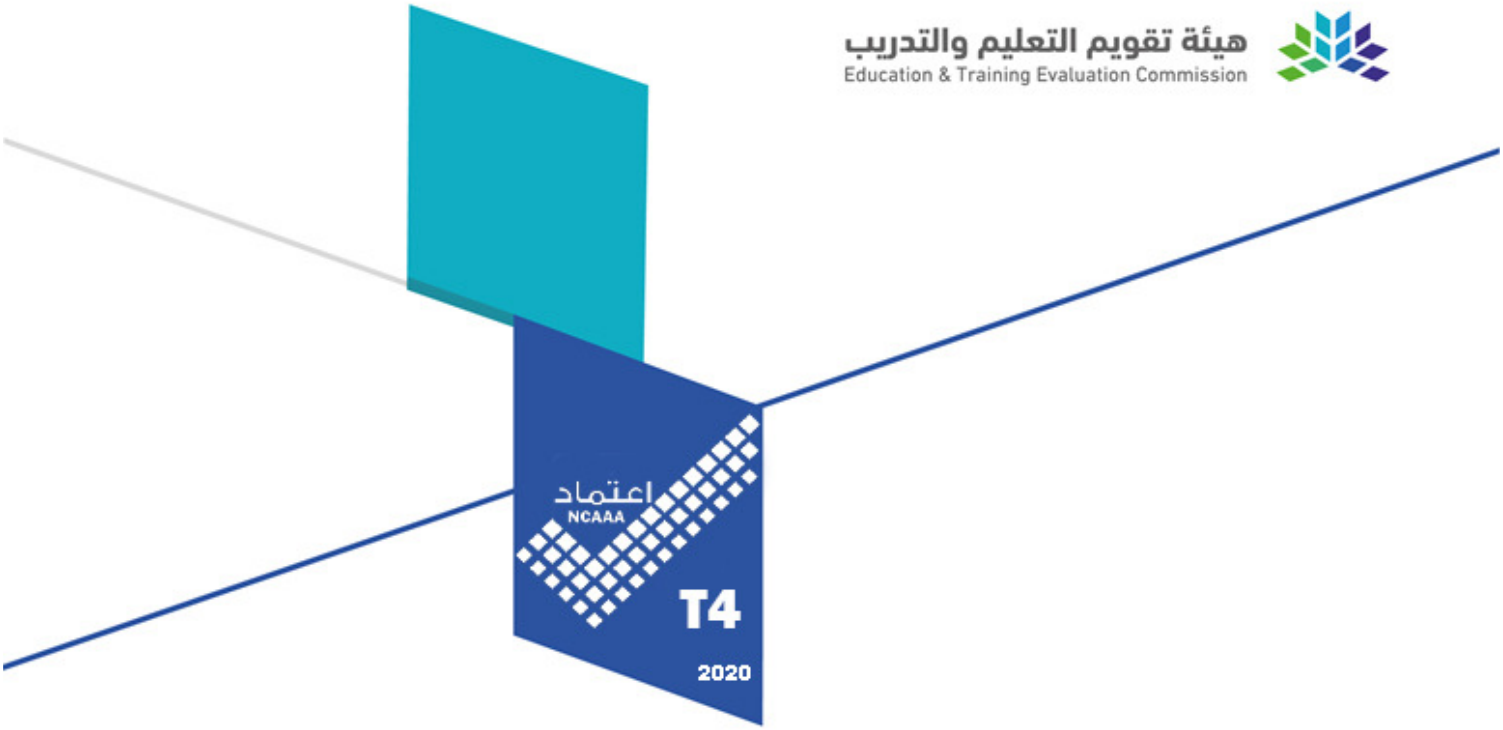

Course Specifications

Course Title:	Software Security Design
Course Code:	IT 464
Program:	Information Technology
Department:	Information Technology
College:	CCIS
Institution:	Majmaah University

Table of Contents

A. Course Identification **3**

6. Mode of Instruction (mark all that apply) 3

B. Course Objectives and Learning Outcomes **3**

1. Course Description 3

2. Course Main Objective 3

3. Course Learning Outcomes 4

C. Course Content **4**

D. Teaching and Assessment **5**

1. Alignment of Course Learning Outcomes with Teaching Strategies and Assessment Methods 5

2. Assessment Tasks for Students 5

E. Student Academic Counseling and Support **5**

F. Learning Resources and Facilities **5**

1.Learning Resources 6

2. Facilities Required 6

G. Course Quality Evaluation **6**

H. Specification Approval Data **6**

A. Course Identification

1. Credit hours **(3, 1, 0)**
2. Course type **a.** University [x] College [ ] Department [ ] Others [ ] **b.** Required [ ] Elective [x]
3. Level/year at which this course is offered: 9
4. Pre-requisites for this course (if any)**:** Cyber Security Findamentals
5. Co-requisites for this course (if any)**:**

6. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	**Traditional classroom**	44	100%
2	**Blended**		
3	**E-learning**		
4	**Distance learning**		
5	**Other**		

7. Contact Hours (based on academic semester)

No	Activity	Contact Hours
1	**Lecture**	33
2	**Laboratory/Studio**	11
3	**Tutorial**	
4	**Others** (specify)	
	Total	44

B. Course Objectives and Learning Outcomes

1. Course Description

This course will provide students to understand the theories and tools used for secure software design, threat analysis, secure coding, and vulnerability analysis. Students will study, in-depth, vulnerability classes to understand how to protect software and how to develop secure software. This course will also cover various analysis and design techniques for improving software security.

2. Course Main Objective

- Understand the theories and tools used for secure software design, threat analysis, secure coding, and vulnerability analysis
- Analyze secure software design and post-implementation security success factors, deliverables, and metrics

- Identify the nature and challenges of Software Security
- Understand the relationship between policy and security
- Apply various methodologies and technologies for Software Assurance
- Analyze vulnerability analysis and Intrusion Detection

3. Course Learning Outcomes

CLOs		Aligned PLOs
1	**Knowledge and Understanding**	
1.1	Describe the risks, threats, and vulnerabilities associated with the transformed digital world	K1
1.2	Understand how to protect software and how to develop secure software	K1
1.3		
1...		
2	**Skills :**	
2.1	Address issues in Web applications Security and technologies	S4
2.2	Apply code auditing practices, and analyze vulnerabilities in memory management	S2
2.3		
3	**Values:**	
3.1		
3.2		

C. Course Content

No	List of Topics	Contact Hours
1	Discussion of the risks, threats, and vulnerabilities associated with the transformation to a digital world, including a look at how business, government, and individuals operate today	6
2	Code auditing: theory, practice, proven methodologies, and secrets of the trade	3
3	Bridging the gap between secure software design and post-implementation review	6
4	Performing architectural assessment: design review, threat modeling, and operational review	6
5	Analyzing vulnerabilities related to memory management, data types, and malformed data	3
6	Evaluating network software: IP stacks, firewalls, and common application protocols	4
7	Analyze Web applications Security and technologies	6
8	Outlines a holistic business-savvy SDL framework that includes people, process, and technology	3
9	Highlights the key success factors, deliverables, and metrics for each phase of the SDL	3
10	Study the most recent updates in Information Systems Security laws, certificates, standards, amendments, and the proposed Federal Information Security Amendments	4
Total		44

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	Describe the risks, threats, and vulnerabilities associated with the transformed digital world	Classroom Teaching	Quiz, Assignment, Mid Exam, Final Exam
1.2	Understand how to protect software and how to develop secure software	Classroom Teaching	Quiz, Assignment, Mid Exam, Final Exam
…			
2.0	**Skills**		
2.1	Address issues in Web applications Security and technologies	Classroom Teaching	Assignment, Final Exam, Lab Based Exercises
2.2	Apply code auditing practices, and analyze vulnerabilities in memory management	Classroom Teaching	Assignment, Final Exam, Lab Based exercises
…			
3.0	**Values**		
3.1			
3.2			
…			

2. Assessment Tasks for Students

#	Assessment task*	Week Due	Percentage of Total Assessment Score
1	Quizzes	4, 8	10%
2	Mid Term Exam	6	20%
3	Assignment	3, 5, 9	10%
4	Lab Based Exercises	Weekly	
5	Final Exam	12	40%
6			
7			
8			

***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 :

Each student is allotted to an academic advisor for guidance and counselling

- Available for a minimum of 4 hours per week/course, as communicated to the students.
- Student also contacts through social networking websites / D2L/ Email for advice and consultations

F. Learning Resources and Facilities

1.Learning Resources

Required Textbooks	1. Cyber Security Engineering: A Practical Approach for Systems and Software Assurance (SEI Series in Software Engineering) 1st Edition , Nancy R. Mead and Carol Woody, Addison-Wesley Professional, 2017. 2. Principles of Computer Security, Fourth Edition, Wm. Arthur Conklin and at el., McGraw-Hill Education, 2015
Essential References Materials	3. Computer Security: Art and Science (2 Volume Set) 1st Edition, Matt Bishop, Addison-Wesley Professional, 2015
Electronic Materials	
Other Learning Materials	

2. Facilities Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	Classroom, PC Laboratory
Technology Resources (AV, data show, Smart Board, software, etc.)	PC or Laptop with Windows/Linux, Smart Board, Projector
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Final Exam Answer Scripts Verification	Peer faculty members	Review
Course Learning Outcomes Feedback	Students	Survey
Final Exam evaluation	Students	Survey

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	