جامعة الـزيتـونــــة الأردنيــة

Al–Zaytoonah University of Jordan

كلية العلوم وتكنولوجيا المعلومات

Faculty of Science and Information Technology

	" عراقة وجودة" "Tradition and Quality"

Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department

QF01/0408-4.0E

Study plan No.	**2024/2025**	**University Specialization**	**Cybersecurity**
Course No.	**0133421**	**Course name**	**Software Security**
Credit Hours	**3**	**Prerequisite Co-requisite**	Software Development Life Cycle
Course type	☐ MANDATORY ☐ UNIVERSITY REQUIREMENT UNIVERSITY ELECTIVE REQUIREMENTS	☐ FACULTY ☐ Support MANDATORY REQUIREMENT course family requirements	☐ Elective ☐ ✓**Mand**requirements **atory requirements**
Teaching style	☐ **Full online learning**	☐ ✓Blended learning	☐ Traditional learning
Teaching model	☐ 2Synchronous: 1asynchronous	☐ 2 face to face : 1synchronous	☐ **3 Traditional**

Faculty member and study divisions information (to be filled in each semester by the subject instructor)

Name	Academic rank	Office No.	Phone No.	E-mail	
Dr. Adi El-Dalahmeh	Assistant Professor	114		A.eldalahmeh@zuj.edu.jo	
Division number	**Time**	**Place**	**Number of students**	**Teaching style**	**Approved model**

Brief description

The Software Security course provides students with a comprehensive overview of the Software Development Life Cycle (SDLC) from a security perspective. It covers the various phases of the SDLC, emphasizing key security aspects, countermeasures, considerations, and industry standards essential for secure software development.

Learning resources

Course book information (Title, author, date of issue, publisher ... etc)	1. CSSLP Certification All-in-One Exam Guide, Third Edition, Wm. Arthur Conklin and Daniel Shoemaker 2022			
Supportive learning resources (Books, databases, periodicals, software, applications, others)	-			
Supporting websites	https://www.eccouncil.org/			
The physical environment for teaching	☐ **Class room**	☐ labs	☐ **Virtual educational platform**	☐ Others
Necessary equipment and software	Tools and software required for conducting digital forensic tasks, along with platforms used for digital forensic activities.			
Supporting people with special needs				
For technical support	**E-learning and Open Educational Center. Computer Center**			

Security Department

Course learning outcomes (S= Skills, C= Competences K= Knowledge,)

No.	Course learning outcomes	The associated program learning output code
	Knowledge	
K1	Basic Knowledge about Software Development Life Cycle SDLC	**MK1**
K2	Know and explain types of security relevant standards.	**MK2**
K3	Knowledge of data and data classification and their relation to security fulfilment along SDLC.	**MK3**
K4	Explain some techniques on how to secure software along the SDLC	**MK4**
	Skills	
S1	Perform a full cycle of threat modelling process.	
S2	Being able to differentiate between different IT systems architectures.	
S3	Being able to implement elementary securing activities along SDLC by following security design principles.	
S4	Clarify concepts for secure coding practices.	
	Competences	
C1	Independently manage tasks related to the security of SDLC.	

Mechanisms for direct evaluation of learning outcomes

Type of assessment / learning style	Fully electronic learning	Blended learning	Traditional Learning (Theory Learning)	Traditional Learning (Practical Learning)
First exam	0	**0**	0	0
Second / midterm exam	%30	**%30**	%30	%30
Participation / practical applications	0	**0**	0	0
Asynchronous interactive activities	%30	**%30**	%30	%30
final exam	%40	**%40**	%40	%40

Note: Asynchronous interactive activities are activities, tasks, projects, assignments, research, studies, projects, work within student groups ... etc, which the student carries out on his own, through the virtual platform without a direct encounter with the subject teacher.

Schedule of simultaneous / face-to-face encounters and their topics

Week	Subject	learning style*	Reference **
1	Software Requirements	Secure Software Requirements	
2	Use case diagram	Use case diagram and misuse cases	
3	Regulation and Compliance	Regulation and Compliance	
4	Data Classification	Privacy	
5	System analysis and Threat Modelling	System analysis and Threat Modelling	
6	System analysis and Threat Modelling	System analysis and Threat Modelling	
7	Threat hunting and attack graph	Threat hunting and attack graph	
8	Mid Term Exam		
9	Define the Security Architectur es	Define the Security Architectures	
10	Define the Security Architectures	Secure Software Design	

11	Secure Software Design	Secure Software Design	
12	Secure Software Design	Secure Coding Practices	
13	Secure Coding Practices	Secure Coding Practices	
14			
15			
16			

*** Learning styles: Lecture, flipped learning, learning through projects, learning through problem solving, participatory learning ... etc.**

**** Reference: Pages in a book, database, recorded lecture, content on the e-learning platform, video, website ... etc.**

Schedule of asynchronous interactive activities (in the case of e-learning and blended learning)

Week	Task / activity	Reference	Expected results
1	Case Study: Identifying Security Requirements in SDLC	Conklin, W.A. & Shoemaker, D. (2022). *CSSLP Certification All-in-One Exam Guide.*	tudents will analyze a sample project and identify critical security requirements for each SDLC phase.
2	Hands-on: Modeling Use Cases and Misuse Cases	Conklin, W.A. & Shoemaker, D. (2022). *CSSLP Certification All-in-One Exam Guide.*	Students will create both use and misuse case diagrams to visualize legitimate and malicious interactions with a system.
3	Exercise: Evaluating Legal and Compliance Standards (ISO, GDPR, PCI-DSS)	Conklin, W.A. & Shoemaker, D. (2022). *CSSLP Certification All-in-One Exam Guide.*	Students will compare major compliance frameworks and summarize their security implications in software projects.
4	Activity: Data Classification and Sensitivity Mapping	Conklin, W.A. & Shoemaker, D. (2022). *CSSLP Certification All-in-One Exam Guide.*	Students will classify datasets by sensitivity and define appropriate protection levels for each class.
5	Practical: Building a Threat Model using STRIDE	Conklin, W.A. & Shoemaker, D. (2022). *CSSLP Certification All-in-One Exam Guide.*	Students will identify and document threats using STRIDE methodology and propose mitigations.
6		Conklin, W.A. & Shoemaker, D. (2022).	Students will perform attack surface enumeration

	Lab: Attack Surface Analysis	*CSSLP Certification All-in-One Exam Guide.*	for a small web application and propose ways to reduce exposure.
7	Simulation: Threat Hunting using Attack Graphs	Conklin, W.A. & Shoemaker, D. (2022). *CSSLP Certification All-in-One Exam Guide.*	Students will model a hypothetical attack chain using an attack graph and identify defensive controls at each node.
8	Mini Project: End-to-End Secure SDLC Case Study	Conklin, W.A. & Shoemaker, D. (2022). *CSSLP Certification All-in-One Exam Guide.*	Students will document a full secure SDLC workflow—from requirements to secure deployment—and present findings.