QF01/0408-4.0E	Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Department

Study plan No.	**2020/2021**		**University Specialization**		**IT**		
Course No.	**0114495**		**Course name**		**Software Security**		
Credit Hours	**3**		**Prerequisite Co-requisite**		**0114213**		
Course type	☐ MANDATORY UNIVERSITY REQUIREMENT	☐ UNIVERSITY ELECTIVE REQUIREMENTS	☐ FACULTY MANDATORY REQUIREMENT	☐ Support course family requirements	✓ Mandatory requirements	☐ Elective 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	
Division number	**Time**	**Place**	**Number of students**	**Teaching style**	**Approved model**

Brief description

This course we will explore the foundations of software security. We will consider important software vulnerabilities and attacks that exploit them -- such as buffer overflows, SQL injection, and session hijacking -- and we will consider defenses that prevent or mitigate these attacks, including advanced testing and program analysis techniques. Importantly, we take a "build security in" mentality, considering techniques at each phase of the development cycle that can be used to strengthen the security of software systems.

يُعرض في هذا المساق أسس أمن البرمجيات. ويعرض كذلك الثغرات الأمنية والبرمجيات الهامة والهجمات التي تستغلها - مثل **buffer overflows**، **SQL injection**، و**session hijacking** وسننظر في الدفاعات التي تمنع هذه الهجمات أو تخففها ، بما في ذلك تقنيات الاختبار المتقدمة وتحليل البرامج. الأهم من ذلك، أننا نأخذ عقلية **"build security in"** "مع الأخذ في الاعتبار التقنيات في كل مرحلة من مراحل دورة التطوير التي يمكن استخدامها لتعزيز أمان أنظمة البرامج.

Learning resources

Course book information (Title, author, date of issue, publisher ... etc)	Core software security: Security at the source. Auerbach Publications Ransome, J., & Misra, A. (2019).			
Supportive learning resources (Books, databases, periodicals, software, applications, others)	1- Software security engineering: a guide for project managers, Mead, N. R., Allen, J. H., Barnum, S., Ellison, R. J., & McGraw, G. R. (2004). Addison-Wesley Professional. 2- IEEE Security & Privacy 2.2, McGraw, Gary. "Software security (2004) 3- Building secure software: How to avoid security problems the right way, portable documents, Viega, J., & McGraw, G. R. (2001), Pearson Education.			
Supporting websites				
The physical environment for teaching	✓ Class room	☐ labs	☐ Virtual educational	☐ Others

			platform	
Necessary equipment and software				
Supporting people with special needs				
For technical support				

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

No.	Course learning outcomes	The associated program learning output code
	Knowledge	
K1	recognize principles of software security	**MK2**
K2	Recognize various software security tools, techniques that could be used to develop a score software	**MK2**
	Skills	
S1	Use software security tools, techniques, and skills to effectively develop a score software	**MS1**
	Competences	
C1	Apply security techniques for different types of software	**MC2**

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)
Midterm exam	30%	30%	**40%**	30%
Participation / practical applications	0	0	**10%**	30%
Asynchronous interactive activities	30%	30%	**0**	0
Final exam	40%	40%	**50%**	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	**Introduction** The Importance and Relevance of Software Security Software Security and the Software	**Lecture**	**Chapter 1**

	Development Lifecycle Quality Versus Secure Code		
2	**Introduction** The Three Most Important SDL Security Goals Threat Modeling and Attack Surface Validation	**Lecture**	**Chapter 1**
3	**The Secure Development Lifecycle** Overcoming Challenges in Making Software Secure Software Security Maturity Models ISO/IEC 27034—Information Technology—Security Techniques—Application Security Security Software Assurance Program Computer Vulnerabilities and Exposures Security and Information Systems Information Analysis Center (CSIAC)	**Lecture**	**Chapter 2**
4	**The Secure Development Lifecycle** Critical Tools and Talent Principles of Least Privilege Privacy The Importance of Metrics Mapping the Security Development Lifecycle to the Software Development Lifecycle Software Development Methodologies Waterfall Development Agile Development	**Lecture**	**Chapter 2**
5	**Security Assessment (A1): SDL** Activities and Best Practices Software Security Team Is Looped in Early Software Security Hosts a Discovery Meeting Software Security Team Creates an SDL Project Plan	**Lecture**	**Chapter 3**
6	**Security Assessment (A1): SDL** Privacy Impact Assessment (PIA) Plan Initiated Security Assessment (A1) Key Success Factors and Metrics Key Success Factors	**Lecture**	**Chapter 3**

	Deliverables Metrics		
7	**Architecture (A2): SDL Activities and Best Practices** A2 Policy Compliance Analysis SDL Policy Assessment and Scoping Threat Modeling/Architecture Security Analysis Threat Modeling Data Flow Diagrams Architectural Threat Analysis	**Lecture**	**Chapter 4**
8	**Architecture (A2): SDL Activities and Best Practices** Ranking of Threats Risk Mitigation Open-Source Selection Privacy Information Gathering and Analysis Key Success Factors and Metrics Key Success Factors Deliverables Metrics	**Lecture**	**Chapter 4**
9	**MIDTERM EXAM (40%)**		
10	**Design and Development (A3): SDL Activities and Best Practices** A3 Policy Compliance Analysis Security Test Plan Composition Threat Model Updating Design Security Analysis and Review	**Lecture**	**Chapter 5**
11	**Design and Development (A3): SDL Activities and Best Practices** Privacy Implementation Assessment Key Success Factors and Metrics Key Success Factors Deliverables Metrics	**Lecture**	**Chapter 5**
12	**Design and Development (A4): SDL Activities and Best Practices** A4 Policy Compliance Analysis Security Test Case Execution Code Review in the SDLC/SDL Process	**Lecture**	**Chapter 6**
13	**Design and Development (A4): SDL Activities and Best Practices** Security Analysis Tools	**Lecture**	**Chapter 6**

	Static Analysis Dynamic Analysis Fuzz Testing Manual Code Review Key Success Factors Deliverables Metrics		
14	**Ship (A5): SDL Activities and Best Practices** A5 Policy Compliance Analysis Vulnerability Scan Penetration Testing Open-Source Licensing Review	**Lecture**	**Chapter 7**
15	**Ship (A5): SDL Activities and Best Practices** Final Security Review Final Privacy Review Key Success Factors Deliverables Metrics	**Lecture**	**Chapter 7**
16	**FINAL EXAM**		

*** 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			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			