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

Study plan No.	**1**		**University Specialization**	**Cybersecurity**	
Course No.	**0125232**		**Course name**	**Data and Information Security**	
Credit Hours	**3**		**Prerequisite Co-requisite**	**Principles of Cybersecurity**	
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	
Hani Mahmoud Almimi	**Assistant Prof.**			**Hani.mimi@zuj.edu.jo**	
Division number	**Time**	**Place**	**Number of students**	**Teaching style**	**Approved model**

Brief description

This course gives introduction about organization assets, information, data, intellectual property, risk management. It describe IT threats and solutions such as Antiviruses, Backups, encryption, security protocols, encryption software, and RAID technology. It describes the key security requirements of confidentiality, integrity, and availability and discuss the types of security threats and attacks. A brief introduction about symmetric and asymmetric encryption, DES, Triple DES, AES is given. The use of secure hash functions for message authentication is also discussed. Moreover, this course presents an overview of the digital signature mechanism, digital certificates, and explain the concept of digital envelopes. It also gives a practical application of encrypting stored data. An overview of VPN is presented. On the other hand, a database and data center security is discussed to understand the unique need for database security, separate from ordinary computer security measures and present an overview of the basic elements of a database management system and relational database system. The course define and explain SQL injection attacks. The database access control is explained and the use of encryption in a database system is discussed.

Learning resources

Course book information (Title, author, date of issue, publisher ... etc)	William Stallings and Lawrie Brown .Computer Security Principles and Practice, Pearson Education Limited (2018)
Supportive learning resources	1- Charles J . Brooks, Christopher Grow, Philip Craig, and Donald Short Sirapat. Cybersecurity essentials. Sybex (2018)

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

(Books, databases, periodicals, software, applications, others)	2- Andy Gill. Into information security. Lean Pub. (2021). 3- Information Technology An Introduction for Today's Digital World, Richard Fox, Second Edition, 2021.			
Supporting websites				
The physical environment for teaching	✓ Class room	☐ labs	✓ Virtual educational platform	☐ Others
Necessary equipment and software	Data show			
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	Knowledge of computer security concepts	**MK1, MK2**
K2	Know, explain and compare types of cryptographic tools	**MK1, MK2**
K3	Knowledge of data and data center security	**MK1, MK2**
K4	Describe IT threats and solutions such as Antiviruses, Backups, encryption, security protocols, encryption software, and RAID technology	**MK1, MK2**
	Skills	
S1	Apply OS installation on Virtual machine and configure users and permissions.	**MS5**
S2	Clarify common security and encryption concepts	**MS1**
S3	Implement encryption to the stored data	**MS3**
S4	Clarify the main concepts in database security.	**MS1**
S5	Explain the some concepts about digital certificates and RAID technology	**MS5**
	Competences	
C1	Independently manage tasks related to data and information security	**MC1**
C2	Work collaboratively and constructively	**MC1**
C3	Have the ability to lead and entrepreneurially perform a wide range of tasks responsibly	**MC2**
C4	Make constructive decisions in situations that require self-reliance	**MC2**
C5	Learn and innovate independently	**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)
First exam	0	**0**	%20	0
Second / midterm exam	%30	**%30**	%20	30%

Participation / practical applications	0	**0**	10	30%
Asynchronous interactive activities	%30	**%20**	0	0
final exam	%40	**%50**	%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	Computer Security Concepts Information, data and intellectual property	Lecture, Activity, Group work, Searching, Practical Implementation	TB ch01, ref03
2	Risk management Threats, Attacks, and Assets	Lecture, Activity, Group work, Searching, Practical Implementation	TB ch01, ref03
3	It threats and solutions: Unauthorized Access and Password Cracking,	Lecture	TB ch01, ref03
4	Malware, Anti-viral software, backups, encryption, encryption software, RAID technology	Lecture	TB ch01, ref03
5	Cryptographic tools: Symmetric encryption, DES, Triple DES, AES, Block vs Stream cipher	Lecture	TB ch02
6	Message Authentication, cryptographic hash function, Asymmetric Encryption	Lecture	TB ch02
7	Algorithms, digital signatures, public certificates,	Lecture, Activity, Group work, Searching, Practical Implementation	TB ch02
8	digital envelope Practical Application: Encryption of Stored Data	Lecture	TB ch02
9	Virtual private network	Lecture, Activity, Group work,	TB ch02, Internet

		Searching, Practical Implementation	
10	review Midterm Exam	Problem solving	
11	Database and Data Center Security	Lecture, Activity, Group work, Searching, Practical Implementation	TB ch05
12	Database security, relational databases, SQL and SQL access controls, DB access control	Lecture	TB ch05
13	Rule-based access control, DB encryption, data security center, SQL	Lecture, Activity, Group work, Searching, Practical Implementation	TB ch05
14	Injection attack.	Lecture, Practical implementation	TB ch05, Internet
15	Revision		
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
2	Activity 1: OS Installation	Supporting material	Installing windows 10 pro on virtual machine
3	Activity 2: Administering Windows 10	Supporting material	Creating users, explore user's groups, explore windows services and task manager, windows PowerShell, view event viewer contents
7	Activity 3: Certificates	Supporting material	Certificate Authority, Types of SSL Certificates,
9	Activity 4: Windows BitLocker	Supporting material	Apply encryption to local drive or external storage using BitLocker
11	Activity 5: RAID technology	Supporting material	Understand the concept of RAID and know their different types
13	Activity 6: Data Backup	Supporting material	Know the types of backups and how to create backups. Know the backup tools?