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

Study plan No.	**2021/2022**		**University Specialization**		**Cybersecurity**
Course No.	**0125231**		**Course name**		**Principles of Cybersecurity**
Credit Hours	**3**		**Prerequisite Co-requisite**		**Introduction to Information Technology**
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

Cybersecurity is defined as the steps and processes taken to protect networks, devices, programs, and data from unauthorized access that can result in theft or damage. Small and large companies alike put cybersecurity measures into place to protect their network, as well as to restrict employees from visiting websites that may compromise sensitive data. This course introduces the concepts and understanding of the field of computer security and how it relates to other areas of information technology. In this class, students receive instruction focused on introductory concepts in cybersecurity. These concepts include cybersecurity theory and basic techniques for optimizing security on personal computers and small networks, security threats, hardening systems.

Learning resources

Course book information (Title, author, date of issue, publisher ... etc)	Security+ Guide to Network Security Fundamentals, Sixth Edition by Mark Ciampa 2018			
Supportive learning resources (Books, databases, periodicals, software, applications, others)	• Cyber Security Threats and Responses for Government and Business by Jack Caravelli and Nigel Jones, 2019 • Cyber-Security and Information Warfare by Nova Science Publishers, Inc. Nicholas J. Daras (Editor), 2019			
Supporting websites				
The physical environment for	☐ **Class**	☐ labs	☐ **Virtual**	☐ Others

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

teaching	**room**		**educational platform**		
Necessary equipment and software					
Supporting people with special needs					
For technical support	**E-learning and Open Educational Center. Computer Center**				

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

No.	Course learning outcomes	The associated program learning output code
	Knowledge	
K1	Explain the challenges of securing information	**MK1**
K2	Define information security and explain why it is important	**MK2**
K3	Identify the types of threat actors that are common today	**MK4**
K4	Describe how to defend against attacks	**MK1**
K5	Define malware and List the different types of malware	**MK5**
K6	Describe the types of psychological social engineering attacks	**MK4**
K7	Explain physical social engineering attacks	**MK1**
	Skills	
S1		
S2		
	Competences	
C1		

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	**%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 to Security Challenges of Securing Information	lecture	Chapter1 (1-10)
2	Reasons for Successful Attacks Difficulties in Defending Against Attacks	lecture	Chapter1 (10-14)
3	What Is Information Security? Understanding Security Defining Information Security	lecture	Chapter1 (14-28)
4	Who Are the Threat Actors? Script Kiddies, Hactivists, Nation State,	lecture	Chapter1 (28-32)
5	Who Are the Threat Actors? Actors, Insiders, Other Threat Actors	lecture	Chapter1(28-32)
6	Defending Against Attacks Fundamental Security Principles	lecture	Chapter1(32-34)
7	Defending Against Attacks Frameworks and Reference Architectures	lecture	Chapter1(34-35)
8	Review Questions	lecture	Chapter1(35-50)
9	Malware and Social Engineering Attacks Mid Exam	lecture	Chapter2(51-55)
10	Attacks Using Malware Circulation	lecture	An enterprise
11	Attacks Using Malware (Infection)	lecture	Chapter2(55-61)
12	Attacks Using Malware Concealment Payload Capabilities	lecture	Chapter2(61-66)
13	Social Engineering Attacks	lecture	Chapter(2) 66-73
14	Social Engineering Attacks Psychological Approaches	lecture	Chapter(2) 75-79
15	Social Engineering Attacks Physical Procedures	lecture	Chapter(2) 79-93
16	Final Exam	lecture	

*** 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	Fill in blanks, drag the words	Lectures 1 and 2	Challenges of Securing Information
2	Fill in blanks, drag the words	Lectures 3 and 4	Difficulties in Defending Against Attacks

3	Fill in blanks, drag the words	Lectures 5 and 6	Understanding Security Defining Information Security
4	Fill in blanks, drag the words	Lectures 7 and 8	Script Kiddies, Hactivists, Nation State,
5	Assignment	Lecture 9 and 10	Actors, Insiders, Other Threat Actors
6	Assignment	Lecture 11 and 12	Fundamental Security Principles
7	Assignment	Lecture 13 and 14	Frameworks and Reference Architectures
8	Assignment	Lecture 9 and 10	Challenges of Securing Information