جامعة عجلون الوطنية Ajloun National University	اسم النموذج : الخطة الدراسية للمادة	رمز النموذج:ك ع 35
	الجهة المصدرة: مشترك بين جميع كليات الجامعة	رقم الاصدار :1
	الجهة المدققة: دائرة الاعتماد وضبط الجودة	
	جهة الإقرار: مجلس العمداء رقم القرار :2023-2022/80 تاريخ القرار:2024/4/26	

Course Description/ School of Information Technology

Department of Cyber Security and Cloud Computing

(Bachelor)

1. Instructor

Instructor's / Coordinator's Name: Dr. Yasser Al-Sharo	
Office Hours: Posted on office door	
Office and Phone: 2021	
Email: yaser.shrah@anu.edu.jo	
Research and Teaching Assistant / Supervisor / Technical (if any): Null	

2. Course Description

This course provides students with the basic information of cybersecurity and information security and its importance. Topics covered in this course include: Introduction to cybersecurity, InformationSecurity, Physical Security, Computer Security, Cyber Crime, Malware and Viruses, Ethical Hacking, Ethics and Legality, Cybersecurity Threats and Attacks, and Introduction to Firewall.

3. Course Information

Level: 1st year	Course Title: Introduction to Cybersecurity	Course No. (314161)
Class Time: Th, Su 17:30-19:00 16:00-17:30	Prerequisite / co-requisite - / (314261), (314262), (314362)	Course Type: Theoretical
Study hours: 3	Semester: First	Academic Year 2025/2026
Type of Teaching: ⊡ Face to Face ⊡ **Blended (**⊡2:1 ⊡1:1 ⊡1:2) **online**		

4. Text Book

Main Reference	Cryptography and Network Security: Principles and Practice
Author	William Stallings
Publisher	**Pearson**
Year	**2022**
Edition	8th
Textbook Website	https://www.amazon.com/Cryptography-Network-Security-Principles-Practice/dp/1292437480/ref=sr_1_2?crid

5. References (books, research published in periodicals or websites)

Serious Cryptography, A Practical Introduction to Modern Encryption, Jean-Philippe,2017.	-1
Cryptography, Steganography and Data Security : Cryptography : Protocols, Design, and Applications Author: Lek, Kamol Rajapakse, Naruemol Publisher: Nova Date Published: 2012	-2

6. Course Learning Outcomes (CLO's))

PLO's	CLO's	
1	Understand and explain basic security concepts in the field of Cybersecurity such as confidentiality, integrity, and availability.	1
2	Explain the importance of Cyberattack, Cybersecurity Threats, Malware for Cybersecurity, Cybersecurity Vulnerabilities	2
4	Identify and explain Ethical Hacking, Penetration tests in Cybersecurity.	3
5	Describe Digital Forensics, firewalls, Webs, and user authentication and authorization.	4
6	Describe securing Internet Protocol (IP) communications by using Internet Protocol Security (IPSec).	5

7. (Curriculum Design Outline Syllabus)

Week:	Subject	:Chapter
1	**Chapter 1: Introduction to Cybersecurity** 1.1 Definition of Security and InfoSec 1.2 Definition of Cybersecurity 1.3 History of Cybersecurity	1
2	1.4. Cybersecurity Objectives (CIA) 1.5 Security Implementation 1.6 Data Ownership 1.7 The Systems Development Life Cycle	1

3	**Chapter 2: Cybersecurity Concepts** 2.1 Cyberattack 2.2 Cybersecurity Threats 2.3 Cybersecurity Vulnerabilities	2
4	2.4 Hackers 2.5 Security Project Team 2.6 Security the Components	2
5	2.7 Most common security mistakes 2.8 Information Security Responsibilities 2.9 Cybersecurity Certificates	2
6	**Chapter 3: Physical and Computer Security** 3.1 Understanding Physical Security 3.2 Physical Security Breach Incidents 3.3 What Is the Need for Physical Security?	3
7	3.4 Who Is Accountable for PhysicalSecurity? 3.5 Factors Affecting Physical Security 3.6 Understanding Computer Security	3
8	**Midterm Exam**	
9	3.7 Principles of Computer Security 3.8 Security Breach 3.9 Types of Threats/Security Attacks	3
10	**Chapter 4: Malware** 4.1 Definition of Malware 4.2 Types of Malware 4.3 Attacks Using Malware	4
11	4.1 Remove Malware 4.2 Preventing infection 4.3 Antivirus	4
12	**Chapter 5: Cyber Crime, Kali Linux, Digital Forensics, Firewall, and Webs** 5.1 Cyber Crime 5.2 Kali Linux	5
13	5.1 Digital Forensics 5.2 Firewall 5.3 Web, Deep Web & Dark Web	5
14	**Chapter 6 Ethical Hacking, Penetration Test** 6.1 Cyber Crime 6.2 Kali Linux	6
15	6.1 Digital Forensics 6.2 Firewall 6.3 Web, Deep Web & Dark Web	6
16	**Final Exam**	

Teaching and learning Strategies and Evaluation Methods

Evaluation /Measurement					Learning Activities	Teaching Strategies	Learning Outcomes	No.
Exam	Quizzes	Home work	Discussion	presentatio				
✓	✓	✓	✓	✓	Lectures , participation, Interaction	Effective Learning	Understand the difference between software security and physical security and discuss ways to improve them of an enterprise.	1
✓	✓	✓	✓	✓	Lectures , participation, Interaction	Effective Learning	Explain the malicious software issues and the use of security tools such as firewalls, intrusion prevention systems.	2
✓		✓	✓	✓	Lectures , participation, Interaction	Effective Learning	Describe the basic process of risk assessment in the context of overall IT security management.	3
	✓	✓	✓	✓	Lectures , participation, Interaction	Effective Learning	Students should be able to ability to encode using traditional and modern methods	4
✓	✓		✓	✓	Lectures, participation, Interaction	Effective Learning	will learn the fundamentals of Cybersecurity, security protocols, authentication protocols, threats penetration tests, digital signatures, key management, and distribution.	5

8. Assessment

Distribution of grades	Assessment Time	Methods Used
%30		**Semester Work**
30%		**Mid Exam**
40%		**Final Exam**

10 .Assessment Relationship to learning Outcomes

CLO_5	CLO_4	CLO_3	CLO_2	CLO_1	Assessment	*No.*
			√	√	**Quiz (1)**	**1**
	√	√			**Quiz (2)**	**2**
			√	√	**Assignment (1)**	**3**
	√	√			**Assignment (2)**	**4**
√	√				**Assignment (3)**	**5**
		√	√	√	**Midterm Exam**	6
√	√	√	√	√	**Final Exam**	7

9. Program Learning Outcomes (PLO's) (To be added by the school)

Applying advanced knowledge, mathematical and algorithmic methods in the fields of computer science.	**1PLO**
Discuss the wide range of principles and tools available for development.	**2PLO**
Building basic databases, how to deal with them, and theoretical and mathematical principles.	**3PLO**
The ability to present ideas, proposals and computerized solutions and discuss them with logical arguments to develop and provide computerized systems that reflect the proposals and ideas presented.	**4PLO**
Describe the wide range of software and hardware used in the development of computer systems.	**5PLO**
Understanding the professional and ethical responsibility related to the specialization.	**6PLO**
Using artificial intelligence methods to solve practical applications.	**7PLO**
Distinguish computer networks, data transmission methods and their basics.	**8PLO**
Using analysis and problem-solving methods.	**9PLO**
Production of educational and application software.	**10PLO**

10. Course Policies

Should be explained to students at the first meeting:

12.1 Class Attendance:

a. Students must attend all classes of this course.
b. Any student with absence of **15%** of the classes of any course, will be illegible to sit for the final exam and will be given the university zero **(35%)** in this course, and the teacher writes the word (deprived, and if a student submits an official sick report authenticated by university clinic or an accepted excuse by the Dean of his/her faculty, the student will be considered as withdrawn from the course.
c. Students are not allowed to come late to classes. Any student coming late will not be allowed to attend the class and he/she will be marked absent.

12.2 Exams: Failure in attending the final exam will result in zero mark unless the student presents an official acceptable excuse to the Dean of his/her faculty who approves an incomplete exam, normally scheduled to be conducted during the first two weeks of the successive semester.

12.3 Assignments & Projects: Assignments and projects should be submitted to the instructor on the due date. Zero mark will be given for late submissions unless the student has an acceptable excuse approved by the instructor of the course.

12.4 Exam Attendance/Punctuality:

a. A student who is late more than 10 minutes will not be permitted to sit the exam (first, second or mid exams).
b. A student who is late more than 30 minutes will not be permitted to sit to final exam, and no student will be permitted to leave the exam center before the elapse of 30 minutes.

12.5 Cheating: Cheating is an attempt to gain marks dishonestly, If the student is caught cheating while taking the exam in one of the courses, or it is proven as a result of the investigation that he attempted to cheat, participated in or attempted to cheat, He shall be collectively punished according to the following:

a. It is considered a failure in that Course.

12.6 Mobiles: Mobile phones should be kept turned off or silent while in class. Usage of mobile phones is not allowed in classes in any form (talking and/or texting).