جامعة الزيتونة الأردنية

Al-Zaytoonah University of Jordan

Course Syllabus

According to JORDAN National Qualification Framework (JNQF)

Course Name: Principles of Cybersecurity and Information Security

Course Number: 0133103

General Course Information:

Course Title	Principles of Cybersecurity and Information Security
Course Number	0133103
Credit Hours	3 credit hours
Education Type	Blended learning
Prerequisites/Co-requisites	Fundamentals of Information Technology
Academic Program	Cybersecurity
Program Code	133
Faculty	Faculty of Information Technology
Department	Cybersecurity
Level of Course	1
Academic Year /Semester	2024/2025 2nd Semester
Awarded Qualification	BS'c
Other Department(s) Involved in Teaching the Course	-
Language of Instruction	English
Date of Production	2024-2025
Date of Revision	

Course Coordinator:

Coordinator's Name	
Office No.	
Office Phone Extension Number	
Office Hours	
E-mail	

Other Instructors:

Instructor Name	
Office No.	
Office Phone Extension Number	-
Office Hours	
Email	

Course Description *(English/Arabic)*:

English	*The Principles of Cybersecurity and information security course provides a foundational understanding of cybersecurity concepts, emphasizing the distinction between cybersecurity and information security, key threats, and strategies for securing systems and networks. Students will explore topics such as cybercrime, security challenges, and techniques for hardening personal computers and small networks. This course combines theoretical knowledge and practical skills to prepare students to address cybersecurity threats and enhance system resilience..*

Arabic	تقدم مادة **مبادئ الأمن السيبراني وأمن المعلومات** فهمًا أساسيًا لمفاهيم الأمن السيبراني، مع التركيز على التمييز بين الأمن السيبراني وأمن المعلومات، والتهديدات الرئيسية، واستراتيجيات تأمين الأنظمة والشبكات. سيستكشف الطلاب موضوعات مثل الجرائم الإلكترونية، تحديات الأمن، وتقنيات تعزيز أمان أجهزة الكمبيوتر الشخصية والشبكات الصغيرة. تجمع هذه الدورة بين المعرفة النظرية والمهارات العملية لإعداد الطلاب لمواجهة تهديدات الأمن السيبراني وتعزيز مرونة الأنظمة.

Textbook: *Author(s), Title, Publisher, Edition, Year, Book website.*

Stallings, W. (2023). *Computer security: Principles and practice.* Pearson Education– 5th edition.

References: *Author(s), Title, Publisher, Edition, Year, Book website.*

1. Security+ Guide to Network Security Fundamentals, Seventh Edition by Mark Ciampa 2022
2. Cyber Security Threats and Responses for Government and Business by Jack Caravelli and Nigel Jones, 2019
3. Cyber-Security and Information Warfare by Nova Science Publishers, Inc. Nicholas J. Daras (Editor), 2019

Course Educational Objectives (CEOs):

CEO1	Demonstrate a comprehensive understanding of the fundamental concepts and principles of cybersecurity and explain the importance of information security.
CEO2	Ability to identify and differentiate various threat actors in the cybersecurity landscape, including script kiddies, hacktivists, nation-state actors, insiders, and other threat actors. They will understand the motivations and tactics of these actors in the context of cyberattacks.
CEO3	Identify and differentiate various types of attacks including malicious software and Social Engineering Attacks

Intended Learning Outcomes (ILO's):

Intended learning outcomes (ILOs)		Relationship to CEOs	Contribution to PLOs	Bloom Taxonomy Levels*	JNQF Descriptors**
K	Knowledge and Understanding				
ILO1-k	Understand the fundamental concepts of cybersecurity and its role in protecting information and systems.	1	1, 2	Understanding	K
ILO2-k	Differentiate between key cybersecurity models, frameworks, and architectures, including NIST, ISO 27001, and Zero Trust Architecture, and their applications.	1	1	Evaluating	K
ILO3-k	Recognize the importance of cybersecurity awareness and training in preventing human errors and mitigating insider threats.	2	1, 3	Analyzing	K
S	Intellectual skills				
ILO4-s	Identify and evaluate common threats, such as malware, social engineering, and vulnerabilities,	3	3	Analyzing	S

	and their impact on individuals and organizations.				
Ilo5-s	Analyze strategies for protecting networks, systems, and data through cryptography, access control, and multi-factor authentication (MFA).	1	4	Applying	S
Ilo6-s	Develop skills to identify and respond to cyberattacks, including early detection, incident response, and vulnerability management.	2	1	Understanding	S
C	Competences				
ILO7-c	Apply strategies and tools to enhance cybersecurity measures, including Security Operations Centers (SOC), security protocols, and preventive measures for malware and social engineering attacks.	2, 3	5	Applying	C

***Bloom Taxonomy Levels:**						
Level #	1	2	3	4	5	6
Level Name	Remembering	Understanding	Applying	Analyzing	Evaluating	Creating
**** Descriptor (National Qualification Framework Descriptors): K: Knowledge, S: Skill, C: Competency.**						

Program Learning Outcome (PLOs):

	(PLOs)	JNQF Descriptors**			
		K	S	C	T
1.	Knowledge of a wide and in-depth range of foundations, theories, principles, and core concepts in the field of cybersecurity.	√			
2.	Knowledge and understanding of analyzing mathematical problems, designing algorithms, evaluating their effectiveness, and knowing various data structures, their uses, advantages, and disadvantages.	√			
3.	The ability to critically assess and select cybersecurity techniques, methodologies, and tools to solve problems, mitigate risks, and perform tasks effectively.		√		
4.	The ability to carry out a wide range of tasks and procedures using cybersecurity tools in various complex operations; to be creative and innovative in this area.		√		
5.	The ability to manage cybersecurity-related tasks independently, work collaboratively and constructively, and possess leadership and entrepreneurial skills while performing a wide range of tasks responsibly.			√	
6.	The ability to make constructive decisions in situations that require self-reliance for work, learning, and innovation independently while adhering to professional ethics and standards.			√	
7.	The ability to work in teams, communicate effectively, and collaborate in a team spirit.				√

** Descriptors according to the national qualifications framework (K: knowledge, S: skill, C: Competency)

Weekly Schedule *(please choose the type of teaching)*

- ☐ **Face to Face (F2F)**
- ☒ **Hybrid** *(One – To - One)*
- ☐ **Online**

Schedule of Simultaneous and their Topics:

Week	First Lecture (F2F)	Second Lecture (Hybrid)	ILOs	PLOs	JNQF Descriptors*
1-2	**Introduction to Cybersecurity** • What is Cybersecurity? • The Difference Between Information Security and Cybersecurity • Cybercrime • The Importance of Cybersecurity • Data Essentials in Cybersecurity: Types, Sensitivity Levels, and Strategic Importance • Cybersecurity on the Web • Cybersecurity in Mobile Devices • The Role of Operating Systems in Enhancing Cybersecurity • Challenges Facing Cybersecurity • Key Cybersecurity Threats • The Importance of Raising Cybersecurity Awareness	Activity on : The Importance of Cybersecurity in digital transformation era	1, 3	1, 2, 3	K

3	**Reasons for Successful Cyber Attacks**
	• Introduction
	• Cybersecurity Lifecycle
	• Human Errors
	• System Vulnerabilities
	• Evolving Attack Techniques
	  • Zero-Day Attacks
	  • spam
	• Poor Access Management
	• Social Engineering Attacks
	• Lack of Security Patches
	• Over-reliance on Technology Without Security Awareness
		Activity on Defending Against Attacks	3, 4	1,3	K, S

4-5	**Information Protection Strategies**
	• Introduction
	• The CIA Triad
	• Information Protection Strategies:
	  • Cryptography
	  • Steganography
	  • Access Control
	  • Multi-Factor Authentication (MFA)
	  • Backup and Data Recovery
	  • Threat Monitoring and Incident Response
	  • Vulnerability Management
	  • Security Awareness and Training
	  • Security Policies and Procedures
	  • Insider Threat Mitigation
	• Challenges Facing Information Protection Strategies
	• Security Operations Center (SOC)
		Activity on :
		• Cryptography
		• Cloud and Endpoint Security
			2	3	K

6	**Physical and Infrastructure Security:** • Introduction • Key Elements of Physical Security • Risks Associated with Physical Security • Strategies to Enhance Physical Security • Examples of Physical Security Incidents	Activity on physical security	2, 3	1, 3	K

7	**Computer Networks Security**
	• Introduction
	• Classifications and Types of Networks:
	  • Geographic Scope
	  • Communication Method
	  • Purpose and Usage
	• Network Layers
	  • OSI Model (Open Systems Interconnection)
	  • TCP/IP Model (Transmission Control Protocol/Internet Protocol)
	• Network Security Tools
	• Network Protection Protocols
	• Key Threats Facing Networks
	• Strategies to Enhance Network Security
		Activity on network security tools	5	7	S

8	**Midterm Exam (30%)**				

9	**Frameworks and Reference Architectures**
	• Introduction
	• Examples of Frameworks and Reference Architectures in Cybersecurity:
	  • NIST Cybersecurity Framework
	  • ISO 27001 Standard
	  • General Data Protection Regulation (GDPR)
	  • HIPAA Standard
	  • Zero Trust Architecture (ZTA) Framework
	• The Importance of Frameworks and Reference Architectures
	• How to Implement Frameworks and Reference Architectures in Organizations
	• Challenges of Implementing Frameworks and Standards
	• Tools for Implementing Frameworks and Standards
		Activity on:
		NIST SP 800-53 Standard, PCI-DSS Standard, and COBIT Framework
			2	1	K

10	**Threat Actors** • Introduction • Types of Threat Actors • Motivations of Threat Actors • Attack Strategies • Defending Against Threat Actors	Activity on Threat Actors	2, 3	1, 3	K, S
11-12	**Attacks Using Malware Circulation** Introduction • Types of Malware • Mechanisms of Malware	Activity on Malware	3, 4, 6	1, 3	S

	Circulation • Network and Application Attacks • Types of Attacks Using Malware Circulation • Concealment Mechanisms of Malware • Risks of Malware Circulation • Strategies to Prevent Malware Circulation • Strategies and tools for Early Detection and Response to Cyber Attacks • Strategies for Preventing Malware • Tools for Detecting and Containing Malware • Practical Examples of Cyberattacks				
14	**Social Engineering :** • Introduction Types of Social Engineering Attacks Psychological Techniques Used in Social Engineering Risks of Social Engineering Attacks Strategies for Preventing Social Engineering Attacks Examples of Social Engineering Attacks	Activity on Social Engineering: Psychological Approaches Activity on Risk Management	4, 7	2, 3	S, C
15	**Projects Discussion**				
	Final Exam				

* **K: Knowledge, S: Skills, C: Competency**

Teaching Methods and Assignments:

Development of ILOs is promoted through the following teaching and learning methods:

- Lecture.
- learning through projects.
- learning through problem solving.
- participatory learning

Course Policies:

A- Attendance policies:
The maximum allowed absences is 15% of the lectures.
B- Absences from exams and handing in assignments on time:
Midterm exam can be retaken based on approval of excuse by the instructor's discretion.
Not handing assignment on time will incur penalties.
C- Academic Health and safety procedures
D- Honesty policy regarding cheating, plagiarism, and misbehaviour:
Cheating, plagiarism, misbehaviour will result in zero grade and further disciplinary actions may be taken.
E- Grading policy:

- All homework is to be posted online through the e-learning system.
- Exams will be marked within 72 hours and the marked exam papers will be handed to the students.
- Online Activities (Course Videos, Practice labs, Discussion Forums, Quizzes) **30%**
- Midterm 30**%**
- Final Exam 40**%**

F- Available university services that support achievement in the course: **E-Learning Platform, Labs, Library.**

Required Equipment:

- PC / Laptop with webcam and mic
- Internet Connection
- Access to the ZUJ E-Learning Platform at https://exams.zuj.edu.jo/
- E-learning plan
- Satisfaction questionnaires for online and face-to-face learning
- Software for e-learning
- Training

Assessment Tools Implemented in the Course:

- Final Exam
- Midterm Exam
- Quizzes
- Homework
- Practice Labs
- Discussion Forums
- Periodic reports for learning assessment
- Improvement plans for online or face-to-face teaching.

Responsible Persons and their Signatures:

Course Coordinator		**Completed Date**	/ /
		Signature	
Received by (Department Head)		**Received Date**	/ /
		Signature	