جامعـة الـزيـتـونـــة الأردنـيـة
Al-Zaytoonah University of Jordan
كلية العلوم وتكنولوجيا المعلومات
Faculty of Science and Information Technology

" عراقة وجودة"
"Tradition and Quality"

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

Study plan No.	**2024/2025**		**University Specialization**		**Cybersecurity**	
Course No.	**0133496**		**Course name**		Selected Topics in Cybersecurity 2	
Credit Hours	**3**		**Prerequisite Co-requisite**		Department Approval	
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 focuses on emerging technologies for transforming cybersecurity by introducing innovative solutions alongside new challenges. Integrating Artificial Intelligence (AI) and Machine Learning (ML) enhances automated threat detection and predictive analytics, enabling organizations to respond to cyber threats in real-time. Additionally, Blockchain technology provides secure decentralized data storage, while the rise of Internet of Things (IoT) devices highlights significant vulnerabilities due to increased connectivity. As advancements like 5G networks expand attack surfaces and quantum computing threatens traditional encryption methods, understanding these technologies is essential for developing robust cybersecurity strategies that effectively address contemporary threats.

Learning resources

Course book information (Title, author, date of issue, publisher ... etc.)	• Course Materials to be provided by the instructor and/or approved textbooks from the department.			
Supportive learning resources (Books, databases, periodicals, software, applications, others)	• Course Materials to be provided by the instructor and/or approved textbooks from the department			
Supporting websites				
The physical environment for teaching	□ ✓**Class room**	□ ✓labs	□ **Virtual educational platform**	□ Others

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, MT= Transferable Skills)*

No.	Course learning outcomes	The associated program learning output code
	Knowledge	
K1	**Examine** recent cybersecurity issues and be able to critically analyze the gaps that lead to the situation	**MK1**
K2	**Understand** the current and emerging best practices in cybersecurity, and critical infrastructure verticals.	**MK2**
	Skills	
S1	**Analyze** and evaluate the current and emerging best practices in cybersecurity.	**MK4**
S2	**Evaluate** an organization's cybersecurity posture and be able to devise strategies to improve its status	**MK1**
	Competences	
C1	**Report** on cybersecurity governance and program performance to stakeholders.	**MC1**
C2		**MC2**
	Transferable Skills	
MT1	**Present** cybersecurity solutions in a language understood by stakeholders with no technical background	**MT1**

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**	0	0
Second / midterm exam	%30	**%30**	%30	%30
Participation / practical applications	0	**0**	0	0
Asynchronous interactive activities	%30	**%30**	%30	%30
final exam	%40	**%40**	%40	%40

Note: Asynchronous interactive activities include tasks such as projects, assignments, research, and group work performed through the virtual platform without direct teacher interaction.

Schedule of simultaneous / face-to-face encounters and their topics

Week	Subject	Learning Style*	Reference **
1	○		●
2	○		●
3	○		●
4	○		●
5	○		●
6	○		●
7	○		●
8	○		●
9	○		●
10	○		●
11	○		●
12	○		●
13	○		●
14	○		●
15	○		●
16	○		●

*** 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.**

Project-Based Learning (PBL) Framework for Cybersecurity Strategy

Project 1: Emerging Cybersecurity Framework Adoption Roadmap

Task / Activity	Reference	Expected Results
Research and analyze 3 emerging frameworks (Zero Trust Architecture, NIST CSF 2.0, MITRE D3FEND). Create a comparative analysis matrix evaluating applicability across different organizational sizes (SME vs Enterprise).	NIST SP 800-207 (Zero Trust), MITRE ATT&CK/D3FEND, Cloud Security Alliance Guidelines	A detailed roadmap document with implementation phases, technology requirements, and maturity assessment criteria for adopting modern security frameworks.
Conduct a threat landscape analysis for 2024-2025 focusing on AI-	ENISA Threat Landscape Report, IBM X-Force	Strategic briefing document mapping emerging threats to

Task / Activity	Reference	Expected Results
powered attacks, supply chain vulnerabilities, and cloud security gaps. Present findings with strategic mitigation recommendations.	Threat Intelligence Index, Gartner Top Security Trends	specific controls and countermeasures with implementation priority ratings.
Design a capability maturity assessment tool measuring people, process, and technology dimensions across security domains (identity, endpoint, network, cloud).	CMMI Institute, ISO/IEC 27001:2022, Cybersecurity Capability Maturity Model	Interactive maturity assessment dashboard with automated scoring and gap analysis visualization for organizational leadership.

Project 2: Comprehensive Security Posture Assessment & Transformation Strategy

Task / Activity	Reference	Expected Results
Perform a simulated security assessment for a fictional mid-sized organization across 5 domains: governance, technical controls, incident response, awareness, and third-party risk.	NIST Cybersecurity Framework, CIS Controls v8, COBIT 2019	Comprehensive assessment report with current state analysis, risk scoring matrix, and executive summary highlighting critical vulnerabilities.
Develop a 3-year transformation strategy with sequenced initiatives addressing technical debt, skill gaps, and process deficiencies. Include business case justifications and ROI calculations.	SANS Security Leadership Essentials, Forrester Total Economic Impact™ model	Phased implementation roadmap with budget projections, resource requirements, and key performance indicators for each initiative.

Task / Activity	Reference	Expected Results
Create board-level communication materials including risk heat maps, security investment justifications, and regulatory compliance alignment mapping.	FAIR (Factor Analysis of Information Risk) model, NACD Cyber-Risk Oversight Handbook	Executive dashboard prototype, board briefing deck, and security metrics framework aligned with business objectives and regulatory requirements.

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	●	●	