الملحق 4: وصف المادة الدراسية

MODULE DESCRIPTION FORM

نموذج وصف المادة الدراسية

Module Information معلومات المادة الدراسية					
Module Title	**Cyber security**			**Module Delivery**	
Module Type	**Core**			☒**Theory** ☐**Lecture** ☒**Lab** ☐**Tutorial** ☐**Practical** ☐**Seminar**	
Module Code	**COM 36111**				
ECTS Credits	**3**				
SWL (hr/sem)	**75**				
Module Level	UGIII		**Semester of Delivery**	2	
Administering Department	BSc - COMM		College	Al-Mansour University College	
Module Leader			**e-mail**		
Module Leader's Acad. Title			**Module Leader's Qualification**		
Module Tutor	Name (if available)		**e-mail**	E-mail	
Peer Reviewer Name	Name		**e-mail**	E-mail	
Scientific Committee Approval Date	13-9-2025		**Version Number**	1.0	

Relation with other Modules العلاقة مع المواد الدراسية الأخرى			
Prerequisite module	None	**Semester**	
Co-requisites module	None	**Semester**	
Module Aims, Learning Outcomes and Indicative Contents			

أهداف المادة الدراسية ونتائج التعلم والمحتويات الإرشادية	
Module Objectives أهداف المادة الدراسية	22. Introduce students to the foundational concepts, principles, and terminology of cybersecurity. This includes understanding the importance of protecting information and systems, the evolving threat landscape, and the role of cybersecurity in modern society. 23. Familiarize students with various security policies, standards, and best practices that are relevant to the field of cybersecurity. This includes understanding legal and regulatory requirements, industry frameworks, and international standards related to information security. 24. Explore the principles and techniques of securing computer networks against unauthorized access, attacks, and data breaches. 25. Provide students with knowledge of secure software development practices and methodologies. This involves understanding common software vulnerabilities, secure coding techniques, secure software development lifecycle, and the importance of testing and vulnerability assessments. 26. Introduce students to the fundamentals of incident response and digital forensics. This includes learning how to detect, respond, and recover from cybersecurity incidents, as well as conducting digital investigations and preserving evidence in a legally admissible manner.
Module Learning Outcomes مخرجات التعلم للمادة الدراسية	1. . Gain a comprehensive understanding of the fundamental concepts, principles, and terminology related to cybersecurity, including the importance of protecting information and systems, the evolving threat landscape, and the role of cybersecurity in society. 2. Demonstrate knowledge and comprehension of various security policies, standards, and best practices relevant to cybersecurity, including legal and regulatory requirements, industry frameworks, and international standards related to information security. 3. Apply secure software development practices and methodologies, including understanding common software vulnerabilities, secure coding techniques, secure software development lifecycle, and the importance of testing and vulnerability assessments 4. Apply skills in identifying, assessing, and managing cybersecurity risks, including understanding risk assessment methodologies, threat modeling, risk mitigation strategies, and business continuity planning. 5. Understand and apply ethical and legal considerations associated with cybersecurity, including privacy laws, intellectual property rights, ethical hacking, professional ethics, and the responsibilities of cybersecurity professionals.

	6. Demonstrate awareness and understanding of emerging technologies and trends in cybersecurity, including cloud security, Internet of Things (IoT) security, artificial intelligence (AI) and machine learning in cybersecurity, and securing mobile and wireless networks.
Indicative Contents المحتويات الإرشادية	Indicative content includes the following. • Module 1: Introduction to cybersecurity. [12 hrs] • Module 2: Attacks, concepts and techniques. [12 hrs] • Module 3: Protecting your Data and Privacy. [12 hrs] • Module 4: Protecting the organization. [12 hrs] • Module 5: Legal and Ethical Issues. [12 hrs]
Description	The main strategy that will be adopted in delivering this module is to learn the concept of cyber security and encourage student's participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes, interactive tutorials and by considering types of simple experiments involving some sampling activities that are interesting to the students.

Learning and Teaching Strategies استراتيجيات التعلم والتعليم	
Strategies	• The main strategy that will be adopted in delivering this module is to encourage students' participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes, interactive tutorials and by considering types of simple experiments involving some sampling activities that are interesting to the students.

Student Workload (SWL) الحمل الدراسي للطالب محسوب لـ ١٥ اسبوعا			
Structured SWL (h/sem) الحمل الدراسي المنتظم للطالب خلال الفصل	**63**	**Structured SWL (h/w)** الحمل الدراسي المنتظم للطالب أسبوعيا	**4**
Unstructured SWL (h/sem)	**12**	**Unstructured SWL (h/w)**	**0.8**

الحمل الدراسي غير المنتظم للطالب خلال الفصل		الحمل الدراسي غير المنتظم للطالب أسبوعيا	
Total SWL (h/sem) الحمل الدراسي الكلي للطالب خلال الفصل	**75**		

Module Evaluation

تقييم المادة الدراسية

		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	Quizzes	2	10% (5)	6 and 12	LO #1 to #3 and #4 to #6
	Assignments	2	10% (5)	2 and 13	LO #3 to #6
	Projects / Lab.	1	10% (10)	Continuous	All
	Report	1	10% (10)	13	LO #3, #4 and #6
Summative assessment	Midterm Exam	2hr	10% (10)	9	LO #1 - #5
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)

المنهاج الاسبوعي النظري

	Material Covered
Week 1	Introduction - World of cybersecurity
Week 2	Organizational Data
Week 3	Cyber Attackers
Week 4	Cyberwarfare
Week 5	Module 2: Attacks, concepts and techniques: Analyzing a Cyber Attack
Week 6	Methods of Infiltration

Week 7	Security Vulnerability and Exploits
Week 8	Module 3: Protecting Your Data and Privacy: Protecting Your Devices and Network
Week 9	Data Maintenance
Week 10	Safeguarding Your Online Privacy.
Week 11	Module 4: Protecting the organization: Cybersecurity Devices and Technologies
Week 12	Behavior Approach to Cybersecurity
Week 13	Module 5: Legal and Ethical Issues: Legal Issues in Cybersecurity
Week 14	Security Operations & Incident Management
Week 15	Operating Systems and Virtualization

Delivery Plan (Weekly Lab. Syllabus)

المنهاج الاسبوعي للمختبر

	Material Covered
Week 1	Study of steps to protect your personal computer system by creating User Accounts with Passwords and types of User Accounts for safety and security
Week 2	Study the steps to protect a Microsoft Word Document of different version with different operating system.
Week 3	Study the steps to remove Passwords from Microsoft Word
Week 4	Study various methods of protecting and securing databases
Week 5	Study “How to make strong passwords” and “passwords cracking techniques”
Week 6	Study the steps to hack a strong password.
Week 7	Perform encryption, decryption using the following substitution techniques (i) Ceaser cipher (ii) playfair cipher (iii) Hill Cipher (iv) Vigenere cipher
Week 8	Perform encryption and decryption using following transposition techniques (i) Rail fence (ii) row & Column Transformation
Week 9	Apply DES algorithm for practical applications
Week 10	Apply AES algorithm for practical applications.
Week 11	Implement the Diffie-Hellman Key Exchange algorithm for a given problem
Week 12	Implement the Diffie-Hellman Key Exchange algorithm for a given problem
Week 13	Calculate the message digest of a text using the SHA-1 algorithm.
Week 14	Implement the SIGNATURE SCHEME – Digital Signature Standard
Week 15	Automated Attack and Penetration Tools Exploring N-Stalker, a Vulnerability Assessment Tool

Learning and Teaching Resources

مصادر التعلم والتدريس

	Text	Available in the Library?
Required Texts	• Eric Conrad , Seth Misenar, Joshua Feldman, CISSP® Study Guide , Fourth Edition, 2023 Elsevier Inc.	No
Recommended Texts	• George K. Kostopoulos, "CYBERSPACE and CYBERSECURITY," © 2013 by Taylor & Francis Group, LLC. • James Graham, Richard Howard and Ryan Olson, "Essential Cybersecurity Science," © 2016 O'Reilly Media, Inc.	yes
Websites	None	

Grading Scheme

مخطط الدرجات

Group	Grade	التقدير	Marks %	Definition
Success Group (50 - 100)	**A** - Excellent	امتياز	90 - 100	Outstanding Performance
	B - Very Good	جيد جدا	80 - 89	Above average with some errors
	C - Good	جيد	70 - 79	Sound work with notable errors
	D - Satisfactory	متوسط	60 - 69	Fair but with major shortcomings
	E - Sufficient	مقبول	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX** – Fail	راسب (قيد المعالجة)	(45-49)	More work required but credit awarded
	F – Fail	راسب	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.