	Ministry of Higher Education and Scientific Research - Iraq **Al-Naji University** **College of Engineering** **Department of Cybersecurity Engineering**	

MODULE DESCRIPTOR FORM
نموذج وصف المادة الدراسية

Module Information
معلومات المادة الدراسية

Module Title	INTRODUCTION TO CYBERSECURITY ENGINEERING		**Module Delivery**	
Module Type	CORE		☒ **Theory** ☐ **Lecture** ☐ **Lab** ☐ **Tutorial** ☐ **Practical** ☐ **Seminar**	
Module Code	**CSE1205**			
ECTS Credits	5			
SWL (hr/sem)	125			
Module Level	UG I	**Semester of Delivery**	2	
Administering Department	CSE	**College**	7294	
Module Leader	Musadaq Ahmed	**e-mail**	musadaq.ahmed@alnaji-uni.edu.iq	
Module Leader's Acad. Title	Assist. Lecturer	**Module Leader's Qualification**	Msc	
Module Tutor	None	**e-mail**	None	
Peer Reviewer Name		**e-mail**		
Review Committee Approval		**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 Aims أهداف المادة الدراسية	This course introduces the fundamental concepts of cybersecurity engineering,

	covering key principles, techniques, and tools used to protect information systems. Students will learn about threats, vulnerabilities, and the measures to mitigate risks in various environments.
Module Learning Outcomes مخرجات التعلم للمادة الدراسية	By the end of this course, students will be able to: 1. Understand the fundamental concepts and terminology of cybersecurity. 2. **Identify** common cybersecurity threats and vulnerabilities. 3. **Understand** the principles of risk assessment and management. 4. **Apply** cybersecurity best practices and standards. 5. **Implement** basic security controls and countermeasures. 6. **Analyze** cybersecurity incidents and develop response strategies.
Indicative Contents المحتويات الإرشادية	Indicative content includes the following. **Overview** This covers, Introduction to cybersecurity, concepts, Threats, Attacks, Security Functional Requirements, Fundamental Security Design Principles, Attack surfaces and trees, and Security strategy. **Part One:** **Computer Security Technology and Principles** Cryptographic Tools, User Authentication, Access Control, Database and Data Center Security, Malicious Software, Intrusion Detection, Firewalls and Intrusion Prevention Systems. [24 hrs.] **Part Two:** **Software and System Security** Software Security, Operating System Security, Cloud and IoT Security. [9 hrs.] **Part Three:** **Management Issues** IT Security Management and Risk Assessment, IT Security Controls, Plans, and Procedures. [12 hrs.]

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 lecture discussions, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes and interactive tutorials.

Student Workload (SWL) الحمل الدراسي للطالب			
Structured SWL (h/sem) الحمل الدراسي المنتظم للطالب خلال الفصل	47	**Structured SWL (h/w)** الحمل الدراسي المنتظم للطالب أسبوعيا	3
Unstructured SWL (h/sem) الحمل الدراسي غير المنتظم للطالب خلال الفصل	78	**Unstructured SWL (h/w)** الحمل الدراسي غير المنتظم للطالب أسبوعيا	5
Total SWL (h/sem) الحمل الدراسي الكلي للطالب خلال الفصل	125		

Module Evaluation تقييم المادة الدراسية					
		Time/Number	**Weight (Marks)**	**Week Due**	**Relevant Learning Outcome**
Formative assessment	**Quizzes**	2	10% (10)	5, 10	LO #1, 2, 10 and 11
	Assignments	2	10% (10)	2, 12	LO # 3, 4, 6 and 7
	Projects	1	10% (10)	Continuous	
	Report	1	10% (10)	13	LO # 5, 8 and 10
Summative assessment	**Midterm Exam**	2 hr	10% (10)	7	LO # 1-7
	Final Exam	2hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus) المنهاج الاسبوعي النظري	
	Material Covered
Week 1	Introduction
Week 2,3	Cryptographic Tools
Week 4	User Authentication
Week 5	Access Control

Week 6	Database and Data Center Security
Week 7	Malicious Software
Week 8	Midterm Exam
Week 9	Intrusion Detection
Week 10	Firewalls and Intrusion Prevention Systems
Week 11	Software Security
Week 12	Operating System Security
Week 13	Cloud and IoT Security
Week 14	IT Security Management and Risk Assessment
Week 15	IT Security Controls, Plans, and Procedures

Learning and Teaching Resources مصادر التعلم والتدريس		
	Text	**Available in the Library?**
Required Texts	Computer Security Principles and Practice, by William Stallings and Lawrie Brown, 5th Ed., 2024	No
Reference book	Cybersecurity Essentials" by Charles J. Brooks, Christopher Grow, and Philip Craig., 2018	No
Reference book	Security Engineering: A Guide to Building Dependable Distributed Systems, 2020	No
Reference book		No
Websites	https://mdl.coie-nahrain.edu.iq	

APPENDIX:

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	مقبول بقرار	(45-49)	More work required but credit awarded
	F – Fail	راسب	(0-44)	Considerable amount of work required
Note:				

NB 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.