Ministry of Higher Education and Scientific Research - Iraq
University of Diyala
College of Engineering for Artificial Intelligence Technology
Department of Cybersecurity Engineering

الملحق ٤: وصف المادة الدراسية

MODULE DESCRIPTION FORM

نموذج وصف المادة الدراسية

Module Information معلومات المادة الدراسية					
Module Title	**Cybersecurity Ethics Law and Policy**			**Module Delivery**	
Module Type	**Core**			☒ **Theory** ☒ **Lecture** ☐ **Tutorial** ☐ **Practical** ☐ **Seminar**	
Module Code	**CSE 105**				
ECTS Credits	**5**				
SWL (hr/sem)	**125**				
Module Level	1		**Semester of Delivery**	1	
Administering Department	Cybersecurity Eng.		**College**	College of Artificial Intelligence Engineering Technology	
Module Leader	Hayder Namuq Talib		**e-mail**	haydernamuq@uodiyala.edu.iq	
Module Leader's Acad. Title	Asst. Lect.		**Module Leader's Qualification**	MSc.	
Module Tutor	Name (if available)		**e-mail**	E-mail	
Peer Reviewer Name	Ali N. Albu-Rghaif		**e-mail**	ali.alb-Rghaif@uodiyala.edu.iq	
Scientific Committee Approval Date	10/11/2025		**Version Number**	1.0	

Relation with other Modules العلاقة مع المواد الدراسية الأخرى			
Prerequisite module	None	**Semester**	
Co-requisites module	None	**Semester**	

Ministry of Higher Education and Scientific Research - Iraq
University of Diyala
College of Engineering for Artificial Intelligence Technology
Department of Cybersecurity Engineering

Module Aims, Learning Outcomes and Indicative Contents أهداف المادة الدراسية ونتائج التعلم والمحتويات الإرشادية	
Module Objectives أهداف المادة الدراسية	1. Introduce students to the basic concepts and terminology of cybersecurity. 2. Develop awareness of ethical behavior and responsible use of digital technologies. 3. Explain the nature of cyber threats, cybercrime, and personal data protection. 4. Provide an understanding of national and international cybersecurity laws and policies. 5. Strengthen students' ability to identify ethical dilemmas and make responsible decisions. 6. Build a foundation for more advanced cybersecurity courses in the following semesters.
Module Learning Outcomes مخرجات التعلم للمادة الدراسية	1. Define fundamental cybersecurity concepts, common threats, and basic security terminology. 2. Explain the importance of cyber ethics and ethical behavior in digital environments. 3. Identify key national and international laws and policies related to cybersecurity and data protection. 4. Describe the role of cybersecurity in protecting individuals, organizations, and national infrastructure.
Indicative Contents المحتويات الإرشادية	**Indicative content includes the following.** Introduction to Cybersecurity & Ethics Basic Cyber Ethics, Professional Behavior, Cybercrime Basics. [8 hrs] Privacy and Personal Data Privacy and Personal Data, Intellectual Property, Simple Cases. [6 hrs] National Cybersecurity National Cybersecurity Concepts, International Cyber Rules, Cybersecurity Policies, Ethical Hacking Basics, New Technologies & Risks, Cyber Conflicts. [10 hrs] Course Review + Final Assessment Full revision, preparation for the final exam. [4 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 the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes, homework's and examples. Practical examples helps students to understand the course material.

Student Workload (SWL) الحمل الدراسي للطالب محسوب لـ ١٥ اسبوعا			
Structured SWL (h/sem) الحمل الدراسي المنتظم للطالب خلال الفصل	**33**	**Structured SWL (h/w)** الحمل الدراسي المنتظم للطالب أسبوعيا	**2.2**
Unstructured SWL (h/sem) الحمل الدراسي غير المنتظم للطالب خلال الفصل	**92**	**Unstructured SWL (h/w)** الحمل الدراسي غير المنتظم للطالب أسبوعيا	**6.1**
Total SWL (h/sem) الحمل الدراسي الكلي للطالب خلال الفصل	**100**		

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

Delivery Plan (Weekly Syllabus) المنهاج الاسبوعي النظري	
	Material Covered
Week 1	Introduction to Cybersecurity What cybersecurity means, why it is important, and examples of cyber threats in daily life.
Week 2	Basic Cyber Ethics Simple explanation of right and wrong behavior online, respecting others, and safe digital practices.
Week 3	Professional Behavior What it means to be responsible when using computers, honesty, and avoiding harmful actions online.
Week 4	Cybercrime Basics Simple types of cybercrime (hacking, stealing accounts, scams) and how they affect people.
Week 5	Privacy and Personal Data What personal data is, why privacy matters, and how websites/apps collect information.
Week 6	Intellectual Property Understanding digital ownership — music, videos, software — and why piracy is wrong.
Week 7	Midterm Review + Simple Cases Reviewing previous topics and discussing easy real-life examples of good/bad cyber behavior.
Week 8	National Cybersecurity Concepts Basic idea of how countries protect their networks and why cybersecurity is a national issue.
Week 9	International Cyber Rules Simple introduction to how countries cooperate against global cybercrime.
Week 10	Cybersecurity Policies Why companies and governments create rules to protect systems and data.
Week 11	Ethical Hacking Basics Difference between ethical hackers and malicious hackers; simple examples of responsible disclosure.
Week 12	New Technologies & Risks Easy intro to risks in AI, IoT devices, social media, and modern apps.
Week 13	Cyber Conflicts Simple explanation of cyber warfare, national security, and digital attacks between countries.
Week 14	Course Review
Week 15	Final Assessment
Week 16	**Preparatory week before the final Exam**

Learning and Teaching Resources مصادر التعلم والتدريس		
	Text	**Available in the Library?**
Required Texts	• Charles P. Pfleeger, Shari Lawrence Pfleeger, “Security in Computing,” Latest Edition.	pdf
Recommended Texts	• William Stallings, “Computer Security: Principles and Practice.” • EC-Council, “Ethical Hacking Essentials.”	No
Websites		

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.