MODULE DESCRIPTION FORM

نموذج وصف المادة الدراسية

Module Information معلومات المادة الدراسية					
Module Title	**Data Security Principles**			**Module Delivery**	
Module Type	**Core**			☒ **Theory** ☐ **Lecture** ☐ **Lab** ☒ **Tutorial** ☐ **Practical** ☒ **Seminar**	
Module Code	**Cys1101**				
ECTS Credits	**5**				
SWL (hr/sem)	**125**				
Module Level		UGI	**Semester of Delivery**		1
Administering Department		Cybersecurity	**College**		College of Computer Science & Information Technology
Module Leader	Ihsan Ahmed Mohammed		**e-mail**		ahssan.ahsan@gmail.com
Module Leader's Acad. Title		Lecturer	**Module Leader's Qualification**		PhD
Module Tutor	Ihsan Ahmed Mohammed		**e-mail**		ahssan.ahsan@gmail.com
Peer Reviewer Name		Dr. Ali Kareem	**e-mail**		alialmujab@uowa.edu.iq
Scientific Committee Approval Date		24/12/2025	**Version Number**		V1

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

Department Head Approval **Dean of the College Approval**

Module Aims, Learning Outcomes and Indicative Contents أهداف المادة الدراسية ونتائج التعلم والمحتويات الإرشادية	
Module Objectives أهداف المادة الدراسية	The objective of this module is to provide students with a solid understanding of fundamental concepts and practices in data security. Students will learn to identify security threats and vulnerabilities, apply cryptographic and authentication techniques, implement access controls, and ensure data integrity and privacy. The module also introduces digital forensics, database security, and relevant legal frameworks, enabling students to develop a holistic view of protecting information in modern computing environments.
Module Learning Outcomes مخرجات التعلم للمادة الدراسية	1. The student will learn the Basic cryptography concepts. 2. Knows what a digital investigation is, the sources of digital evidence, and the limitations of forensics. 3. An overview of the concepts of authentication, authorization, access control, and data integrity. 4. Finally, review some of the various techniques for data erasure.
Indicative Contents المحتويات الإرشادية	1. Introduction to Data Security Principles • Fundamental security objectives: confidentiality, integrity, availability (CIA) • Threats, vulnerabilities, and risk concepts • Security controls and defense-in-depth • Organizational and technical perspectives of data protection 2. Basic Cryptography Concepts • Cryptographic primitives: encryption, hashing, digital signatures • Symmetric vs. asymmetric cryptography • Key generation, distribution, and management basics • Use cases: data protection, integrity checks 3. Historical Ciphers • Classical substitution and transposition ciphers • Caesar, Vigenère, and One-Time Pad (concept) • Cryptanalysis basics and evolution toward modern cryptography • Lessons learned from historical weaknesses 4. Digital Forensics • Purpose and scope of digital forensics • Evidence acquisition and chain of custody • Log analysis and incident investigation fundamentals 5. Data Integrity and Authentication • Ensuring data accuracy, consistency, and trustworthiness • Message Authentication Codes (MAC), hashing, checksums • Digital certificates and authentication protocols

	6. Password Storage Techniques and Data Integrity • Secure password hashing: salts, key-stretching (PBKDF2, bcrypt, scrypt) • Password policies and authentication risks • Common attacks: brute force, dictionary, rainbow tables • Maintaining integrity in authentication systems 7. Access Control • Access control models: DAC, MAC, RBAC, ABAC • Privilege escalation risks and mitigation • Session management and authorization processes • Identity and access management (IAM) fundamentals 8. Data Privacy • Principles of data minimization, purpose limitation, and user consent • Personally identifiable information (PII) and sensitive data classification • Privacy-enhancing techniques (pseudonymization, anonymization) • Data privacy risks and common mitigation approaches 9. Information Storage Security • Secure storage methods: encryption at rest, disk/volume encryption • Backup strategies, redundancy, and recovery • Secure deletion, retention, and lifecycle management • Physical storage security considerations 10. Database Security • Threats to databases: SQL injection, privilege abuse, insider attacks • Access control and role-based permissions in DB systems • Encryption of data at rest and in transit • Logging, auditing, and monitoring of database activity 11. Report Seminar • Student-led research presentations on chosen security topics • Development of report writing skills (formatting, referencing) • Critical evaluation of sources and case studies • Peer review and in-class discussion 12. Data Security Law • Overview of national and international data protection regulations • GDPR/ISO27001 principles and compliance obligations • Legal aspects of data breaches and incident reporting • Ethical considerations in handling personal and sensitive data

Learning and Teaching Strategies استراتيجيات التعلم والتعليم	
Strategies	1- Lectures 2- Problem based learning 3- Case studies 4- Feedback and Formative Assessment

Student Workload (SWL) الحمل الدراسي للطالب محسوب لـ ١٥ اسبوعا			
Structured SWL (h/sem) الحمل الدراسي المنتظم للطالب خلال الفصل	48	**Structured SWL (h/w)** الحمل الدراسي المنتظم للطالب أسبوعيا	3
Unstructured SWL (h/sem) الحمل الدراسي غير المنتظم للطالب خلال الفصل	77	**Unstructured SWL (h/w)** الحمل الدراسي غير المنتظم للطالب أسبوعيا	2
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/Attendance**	5	10% (10)	All	1,3
	Assignments	5	10% (10)	4,8,12	3,4
	Onsite Assignments	2	10% (10)	3,5,7,9,14	3
	Reports	2	10% (10)	6,13	all
Summative assessment	**Midterm Exam**	2	10% (10)	7	1,2
	Final Exam	3	50% (50)	16	all
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus) المنهاج الاسبوعي النظري	
	Material Covered
Week 1	Overview about Data Security Principles
Week 2	Introduction to Data Security Principles
Week 3	Basic cryptography concepts
Week 4	Historical ciphers
Week 5	Digital Forensics
Week 6	Data Integrity and Authentication
Week 7	MidTerm Exam
Week 8	Password storage techniques and Data Integrity
Week 9	Access Control
Week 10	Data Privacy
Week 11	Information storage security

Week 12	Database security
Week 13	Report seminar
Week 14	Data security law
Week 15	Preparation for Final Exam

Learning and Teaching Resources
مصادر التعلم والتدريس

	Text	Available in the Library?
Required Texts	Cryptography and Network Security, principles and practice, Global Edition – Eighth Edition, William Stallings, 2023	No
Recommended Texts	https://cybersecurityguide.org/resources/reading-list/#book	No
Websites	https://www.coursera.org/professional-certificates/google-cybersecurity	

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.