



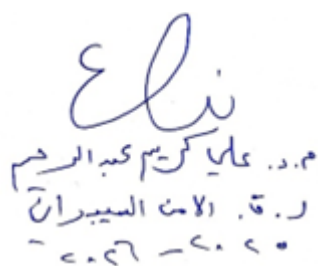
MODULE DESCRIPTION FORM

نموذج وصف المادة الدراسية

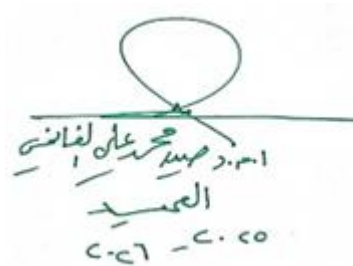


Module Information			
معلومات المادة الدراسية			
Module Title	Cysersecurity Principles		Module Delivery
Module Type	Basic		☒ Theory ☒ Practical
Module Code	cys1201		
ECTS Credits	8		
SWL (hr/sem)	200		
Module Level	UGI	Semester of Delivery	1
Administering Department	Cybersecurity	College	College of Computer Science & Information Technology
Module Leader	M.D.ahssan Ahmed Muhammad	e-mail	ahssan.ahsan@gmail.com
Module Leader's Acad. Title	Assist Lecturer	Module Leader's Qualification	M.Sc
Module Tutor	M.D.ahssan Ahmed Muhammad	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	Cys1101	Semester	1
Co-requisites module	Non	Semester	...


 م.د. علي كريم عبد الرحمن
 ر.ق. الامت السبيران
 ٢٠٢٥ - ٢٠٢٦




 م.د. محمد علي لافان
 العميد
 ٢٠٢٥ - ٢٠٢٦

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	<ol style="list-style-type: none"> 1. Provide students with a solid understanding of database concepts, principles, and established best practices. 2. Introduce students to the fundamentals of database design, implementation, and management. 3. Cover topics such as data modeling, normalization, and query optimization. 4. Develop practical skills in using database management systems and query languages. 5. Foster critical thinking and problem-solving skills within the context of database design and management. 6. Prepare students to apply their knowledge in real-world environments and scenarios. 7. Enable students to contribute to the development of effective database solutions within the IT sector.
Module Learning Outcomes مخرجات التعلم للمادة الدراسية	<ol style="list-style-type: none"> 1. Understand fundamental database concepts and principles, including data models, schemas, and normalization. 2. Demonstrate proficiency in designing, implementing, and managing databases using a Database Management System (DBMS). 3. Apply data modeling techniques to develop logical and physical database designs that meet specific requirements. 4. Create and execute complex SQL queries to retrieve, update, and manipulate data within the database. 5. Evaluate and optimize query performance using indexing, query tuning, and other optimization techniques. 6. Implement and enforce data integrity constraints, including entity relationships, referential integrity, and data validation rules. 7. Employ appropriate security measures to protect data and ensure the confidentiality, integrity, and availability of the database. 8. Utilize backup and recovery procedures to protect data and restore the database in the event of failure or disaster.
Indicative Contents المحتويات الإرشادية	

Learning and Teaching Strategies استراتيجيات التعلم والتعليم	
Strategies	<p>Course Overview and Strategies</p> <p>Cybersecurity is not merely a technical issue but also a human one; individuals play a pivotal role in both the risks associated with cyber threats and the mitigation of those risks. This course provides insights, strategies, and skills to address control vulnerabilities linked to individual behavior within an organization—vulnerabilities that could expose the business to cyber threats.</p>

	<ul style="list-style-type: none"> • It is also crucial to appreciate the significance of people, laws, and ethics in managing cybersecurity programs within organizations. • To effectively manage and protect organizational information assets, students must develop the knowledge and skills required for security planning, as well as for the development, implementation, and evaluation of security policies and programs. • Through a series of lectures, this course equips students with the knowledge, skills, and processes necessary for appropriate response and recovery following the detection of a cybersecurity incident. • Students are introduced to cybersecurity principles and learn how to plan for, detect, respond to, and recover from current and emerging cyber threats. • The course covers vulnerability detection and remediation, encryption techniques, intrusion detection, and cyber risk management. • The application of best practices supporting a robust cybersecurity posture—across software development, systems administration, and information systems professions—is explored through lectures, hands-on laboratory exercises, targeted assignments, and mini-projects.
--	---

Student Workload (SWL)			
الحمل الدراسي للطلاب محسوب لـ ١٥ اسبوعا			
Structured SWL (h/sem) الحمل الدراسي المنتظم للطلاب خلال الفصل	60	Structured SWL (h/w) الحمل الدراسي المنتظم للطلاب أسبوعيا	4
Unstructured SWL (h/sem) الحمل الدراسي غير المنتظم للطلاب خلال الفصل	87	Unstructured SWL (h/w) الحمل الدراسي غير المنتظم للطلاب أسبوعيا	6
Total SWL (h/sem) الحمل الدراسي الكلي للطلاب خلال الفصل	150		

Module Evaluation تقييم المادة الدراسية					
		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	Tests	4	8% (8)	3,6,10,13	1,3
	College duties	6	12% (12)	3,5,6,8,10,12	3,6
	Projects	1	10%(10)	It starts in week 4 Unit 5 in week 14	2,3,6,7
	lab	5	10% (10)	7,13	All
Summative assessment	Midterm Exam	2hr	10% (10)	7	1,2,3
	Final Exam	3hr	50% (50)	16	1,2,3,4,6
Overall rating			100% (100)		

Delivery Plan (Weekly Syllabus) المنهاج الاسبوعي النظري	
	Material Covered
Week 1	<p>Perspectives and Impacts of Cybersecurity Makes implementation a continuous challenge. The essence of cybersecurity Understanding difficult problems The organization's focus on cybersecurity increases revenue Describing how a cyber event caused a problem The field of cybersecurity tells a story about significant progress in</p>
Week 2	<p>Perspectives and Implications of Cybersecurity – Continued</p> <ul style="list-style-type: none"> Assessing breaches of privacy, transparency, or availability (CIA) of information and how this affects trust in information Comparing and evaluating different cryptocurrency methods/applications.
Week 3	<p>Policy Objectives and Mechanisms</p> <ul style="list-style-type: none"> Identifying the organization's approach to security, considering standards, best practices, and the latest technologies. In the context of cybersecurity, it is important to be aware of the multiple definitions of the word "policy." Considering the notification of vulnerabilities and problems related to fixing or not fixing them, and disclosing or not disclosing them.
Week 4	<p>Policy Objectives and Mechanisms – Continued</p> <ul style="list-style-type: none"> Comparing the impact of open design versus confidential design on security.

	<ul style="list-style-type: none"> • Societal imperative: Explaining why cybersecurity is important.
Week 5	<p>Security Services, Mechanisms, and Countermeasures</p> <ul style="list-style-type: none"> • Analyze the balance of key security attributes (precision, vulnerability, and availability) • Understand the concepts of risk, threat, vulnerability, and attack pathways. • Document an example of a countermeasure for identified threats. • Develop a list of tools and capabilities for continuously identifying cyber risks. • Explain the concept of identity management and its importance.
Week 6	<p>Security Services, Mechanisms, and Countermeasures – Continued</p> <p>Access.</p> <p>Understanding the concepts of authentication, authorization, and control</p> <ul style="list-style-type: none"> • Defending the benefits of multi-factor authentication • Access. <p>Explaining authentication, authorization, and control</p> <ul style="list-style-type: none"> • Using biometrics. <p>Explaining the benefits of two-factor authentication, including</p> <ul style="list-style-type: none"> • Defining application whitelisting • Products <p>Identifying the costs and trade-offs associated with implementing security</p>
Week 7	Midterm exam review
Week 8	<p>Vulnerabilities, Threats, and Risks</p> <ul style="list-style-type: none"> • Explain the differences between vulnerabilities, threats, and risks. • Describe how vulnerabilities are contained by security mechanisms. • Use a risk management framework. • Use vulnerability testing tools to identify vulnerabilities. • Explain the benefits of Defense in Depth (DDR) using multiple layers of protection. • Describe how security issues arise at the component boundaries.
Week 9	<p>Vulnerabilities, Threats, and Risks – Continued</p> <ul style="list-style-type: none"> • Installed software using the National Vulnerability Database to identify vulnerabilities in servers or network components. • Identifying vulnerabilities, threats, and risks related to network infrastructure, cloud servers, desktop computers, and mobile devices. • Using a buffer overflow attack on a server. • Using a cross-site scripting attack on a server that does not properly filter user input.
Week 10	<p>Personal Information</p> <ul style="list-style-type: none"> • Understanding the terms: personal information, identifiable information, deidentification, anonymization, pseudonymization, concealment, and disclosure. <p>Describing how Fair Information Practices apply to the collection and use of personal information on the internet.</p> <p>Privacy level and disclosure risks</p> <p>Classifying several categories of personal information according to...</p>
Week 11	<p>Personal Information – Continued</p> <ul style="list-style-type: none"> • Comparing policies for the collection, processing, storage, sharing, and disposal of personal information. • Protecting personal information. • Clarifying the role and limits of transparency. • Understanding policies and techniques for separating personal data from corporate data.

	<ul style="list-style-type: none"> Analyzing methods for controlling access to personal information.
Week 12	<p>Cyber Attacks and Their Detection</p> <ul style="list-style-type: none"> Defining the roles of prevention, deterrence, and detection mechanisms. Identifying password guessing, port scanning, SQL injection attacks, and file and registry infiltration. Discussing the role and limitations of signature-based and behavioral anti-phishing techniques.
Week 13	<p>Cyberattacks and Detection – Continued</p> <ul style="list-style-type: none"> Deploy teams to implement intrusion detection systems on the host and network. Establish three rules for the network intrusion detection system to protect against specific attacks. Discuss the use of deception by malicious software to bypass security mechanisms.
Week 14	<p>Cyber Attacks and Security Tools</p> <ul style="list-style-type: none"> Explaining the concepts of hacking and phishing. Identifying Denial-of-Service (DoS) attacks and spam emails. Types of security tools and tips for protecting against cybercrime. Following the principles of cybersecurity.
Week 15	Assessing the student's workload on the course
Week 16	Final Exam

Learning and Teaching Resources

مصادر التعلم والتدريس

	Text	Available in the Library?
Required Texts	1. Distributed Database Systems – Vera Goebel 2. Distributed Database Management Systems: A Business Approach	yes
Recommended Texts	1. Distributed Database Systems 2. Distributed Systems 3. Principles of Distributed Database Systems 4. Distributed Database Management Systems 5. Management Systems	
Websites	https://www.tutorialspoint.com/distributed_dbms/distributed_dbms_databases.htm What is a distributed database? Definition from TechTarget Principles of Distributed Database Systems SpringerLink	

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.