MODULE DESCRIPTION FORM

نموذج وصف المادة الدراسية

Module Information معلومات المادة الدراسية					
Module Title	**Information Security Technologies**			**Module Delivery**	
Module Type	**Core**			☒ **Theory** ☐ **Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical** ☒ **Seminar**	
Module Code	**IT4101**				
ECTS Credits	**6**				
SWL (hr/sem)	**150**				
Module Level	4		**Semester of Delivery**	1	
Administering Department	Information Technology		**College**	College of Computer Science & Information Technology	
Module Leader	**Ahsan Ahmed Mohammed Lahmood**		**e-mail**	ahssan.ahsan@gmail.com	
Module Leader's Acad. Title	Asst. Prof		**Module Leader's Qualification**	Ph.D.	
Module Tutor	**Ahsan Ahmed Mohammed Lahmood**		**e-mail**	ahssan.ahsan@gmail.com	
Peer Reviewer Name	Nabil Sadiq Abdul abbas		**e-mail**	nabeel.alshreefy@uowa.edu.iq	
Scientific Committee Approval Date	01/09/2026		**Version Number**	1.0	

Relation with other Modules العلاقة مع المواد الدراسية الأخرى			
Prerequisite module	IT3202	**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 Aims أهداف المادة الدراسية	general module aims that could be considered: 1. Introduce the concept of information security: The module aims to provide students with a basic understanding of what information security is and why it is important in today's digital age. 2. Identify potential security risks: Students should learn to recognize common security risks such as malware, phishing attacks, and data breaches. They should understand the consequences of these risks and the importance of protecting sensitive information. 3. Explore password security: The module aims to teach students about the importance of strong and unique passwords. They should learn how to create secure passwords, how to store them safely, and why it is crucial to avoid sharing passwords with others. 4. Introduce online privacy: Students should gain an understanding of the importance of privacy when using digital platforms and the internet. They should learn about the potential risks associated with sharing personal information online and how to protect their privacy. 5. Educate about safe browsing habits: The module aims to teach students about safe browsing practices, including avoiding suspicious websites, understanding website security indicators (e.g., SSL/TLS certificates), and recognizing and avoiding online scams. 6. Introduce antivirus and firewall software: Students should learn about the role of antivirus and firewall software in protecting computer systems from malware and unauthorized access. They should understand how to select and use these tools effectively. 7. Teach responsible social media use: The module aims to educate students about responsible behavior on social media platforms. They should learn about the potential consequences of sharing inappropriate content and the importance of respecting others' privacy online. 8. Address cyberbullying and online harassment: Students should be made aware of the harmful effects of cyberbullying and online harassment. They should learn strategies to respond to and report such incidents, as well as understand the importance of being kind and respectful to others online. 9. Introduce data backup and recovery: The module aims to teach students about the importance of regularly backing up their data and the various methods available for data backup. They should also learn about data recovery options in case of data loss. 10. Promote ethical and responsible technology use: The module aims to foster a sense of digital citizenship and responsibility. Students should learn about the ethical use of technology, including respecting copyright laws, avoiding plagiarism, and understanding the impact of their online actions.

Module Learning Outcomes مخرجات التعلم للمادة الدراسية	1. Identify and explain common security risks: Students should be able to recognize and describe common security risks such as viruses, malware, phishing, and identity theft. 2. Demonstrate knowledge of password security: Students should understand the importance of using strong and unique passwords, and be able to create and remember secure passwords for their digital accounts. 3. Apply safe browsing practices: Students should be able to demonstrate safe browsing habits, including avoiding suspicious websites, recognizing secure websites, and understanding the importance of not clicking on unknown links. 4. Understand the concept of online privacy: Students should grasp the concept of online privacy and be able to identify and explain personal information that should not be shared online. 5. Recognize and respond to cyberbullying: Students should be able to identify instances of cyberbullying and understand how to respond to and report such incidents. 6. Explain the role of antivirus and firewall software: Students should understand the purpose of antivirus and firewall software in protecting computer systems from threats and be able to explain their importance. 7. Practice responsible social media use: Students should understand the importance of respectful behavior on social media platforms, including avoiding sharing inappropriate content and respecting others' privacy. 8. Demonstrate knowledge of data backup and recovery: Students should understand the importance of regularly backing up their data and be able to explain different methods for data backup and recovery. 9. Exhibit ethical technology use: Students should demonstrate an understanding of ethical technology use, including respecting copyright laws, giving credit for digital content, and avoiding plagiarism.
Indicative Contents المحتويات الإرشادية	1. Introduction to Information Security o Understanding the concept of information security o Exploring why information security is important 2. Common Security Risks o Viruses, malware, and their impact o Phishing attacks and how to identify them o Protecting against identity theft 3. Password Security o Creating strong and unique passwords o Password management tools and strategies o The importance of not sharing passwords with others 4. Safe Browsing Habits o Recognizing secure websites (SSL/TLS certificates) o Avoiding suspicious websites and pop-ups o Understanding the risks of clicking on unknown links 5. Online Privacy o Identifying personal information that should not be shared online o Understanding the importance of privacy settings o Safeguarding personal information on social media platforms 6. Cyberbullying and Online Harassment o Recognizing and understanding cyberbullying o Strategies to respond to and report cyberbullying incidents o Promoting a safe and respectful online environment 7. Antivirus and Firewall Software o Introduction to antivirus and firewall software

	o Understanding their role in protecting against threats o Selecting and installing reliable security software 8. Responsible Social Media Use o Posting and sharing appropriate content o Respecting others' privacy and digital citizenship o Understanding the consequences of online actions 9. Data Backup and Recovery o Importance of regular data backup o Methods for backing up data (e.g., external hard drives, cloud storage) o Data recovery options in case of data loss 10. Ethical Technology Use o Respecting copyright laws and intellectual property o Understanding plagiarism and giving credit for digital content o Promoting ethical behavior in online interactions 11. Critical Thinking and Online Information o Evaluating the credibility and reliability of online information o Developing critical thinking skills to make informed decisions o Fact-checking and verifying online information sources
Learning and Teaching Strategies استراتيجيات التعلم والتعليم	

Strategies	1. Interactive Discussions: Engage students in discussions about information security concepts, risks, and best practices. Encourage them to share their thoughts, experiences, and questions related to online safety and privacy. 2. Multimedia Presentations: Utilize multimedia resources such as videos, animations, and interactive presentations to explain complex concepts in a visually appealing and easily understandable manner. These resources can capture students' attention and enhance their understanding. 3. Hands-on Activities: Incorporate hands-on activities to reinforce learning. For example, have students create and practice using strong passwords, identify phishing emails, or differentiate between secure and insecure websites through interactive exercises. 4. Case Studies and Real-Life Scenarios: Present case studies or real-life scenarios that illustrate the importance of information security. Encourage students to analyze and discuss the potential risks and appropriate actions to mitigate those risks. 5. Role-Playing and Scenarios: Engage students in role-playing activities where they can act out different online security situations. For example, they can simulate responding to a phishing email or creating a secure password in a role-playing scenario. 6. Group Projects and Collaborative Learning: Assign group projects where students can collaborate on researching and presenting different aspects of information security. This promotes teamwork, critical thinking, and deeper understanding of the subject matter. 7. Guest Speakers or Experts: Invite guest speakers or experts in the field of information security to share their knowledge and experiences with the students. This provides real-world insights and helps students connect the concepts to practical applications. 8. Gamification: Incorporate educational games or interactive quizzes related to information security to make learning fun and engaging. This approach can reinforce knowledge, encourage healthy competition, and provide immediate feedback. 9. Internet Safety Workshops: Organize workshops or invite local law enforcement or cybersecurity professionals to conduct sessions on internet safety and responsible online behavior. These sessions can provide valuable insights and practical tips for students. 10. Reflection and Evaluation: Encourage students to reflect on their own online behaviors and evaluate the security measures they currently practice. Prompt them to identify areas for improvement and develop personal action plans to enhance their own information security practices

Student Workload (SWL) الحمل الدراسي للطالب محسوب لـ 15 اسبوعا			
Structured SWL (h/sem) الحمل الدراسي المنتظم للطالب خلال الفصل	65	**Structured SWL (h/w)** الحمل الدراسي المنتظم للطالب أسبوعيا	5
Unstructured SWL (h/sem) الحمل الدراسي غير المنتظم للطالب خلال الفصل	85	**Unstructured SWL (h/w)** الحمل الدراسي غير المنتظم للطالب أسبوعيا	6
Total SWL (h/sem) الحمل الدراسي الكلي للطالب خلال الفصل	150		

Module Evaluation
التقييم التكويني للطالب

		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
	Quizzes	5	2 (10%)	2,4,6,7,8,10	1,2,3,4
	Projects	1	5 (5%)	12	All
	Lab	5	3 (15%)	all	All
	H.W	5	2 (10%)	3,5,7,9,11	All
Summative	**Midterm Exam**	2hr	10%(10)	7	
assessment	**Final Exam**	3hr	50% (50)	16	
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)

	Material Covered
Week 1	Introduction to Information Security
Week 2	Common Security Risks
Week 3	Password Security
Week 4	Explain the importance and application of each of confidentiality, integrity, authentication and availability
Week 5	Attacks on Computers and Computer Security:
Week 6	Security Mechanisms, A model for Network Security. Cryptography: Concepts and Techniques:
Week 7	**CONVENTIONAL ENCRYPTION PRINCIPLES**
Week 8	DATA ENCRYPTION STANDARD
Week 9	PUBLIC KEY CRYPTOGRAPHY
Week 10	RSA ALGORITHM
Week 11	DIFFIE-HELLMAN KEY EXCHANGE
Week 12	ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

Week 13	Message Authentication Algorithms and Hash Function:
Week 14	**Online Privacy**
Week 15	**Ethical Technology Use**

Delivery Plan (Weekly Lab. Syllabus)	
	Material Covered
Week 1	Lab 1: Implement Caesar Cipher
Week 2	Lab 2: Implement Affine Cipher with equation c=3x+12
Week 3	Lab 3: Implement Playfair Cipher with key entered by user
Week 4	Lab 4: Implement polyalphabetic Cipher
Week 5	Lab 5: Implement AutoKey Cipher
Week 6	Lab 6: Implement Hill Cipher
Week 7	**Lab 7: Implement Rail fence technique**
Week 8	Lab 8: Implement Simple Columner Transposition technique
Week 9	Lab 9: Implement Advanced Columner Transposition technique
Week 10	Lab 10: Implement Simple RSA Algorithm with small numbers
Week 11	Lab 11: Implement Simplified DES
Week 12	Lab 12: Block Ciphers and the Data Encryption Standard
Week 13	Lab 13: Advanced Encryption Standard
Week 14	**Lab 14: Make a study of one IDS (For ex. Snort**
Week 15	**Lab 15: Exam Revision**

Learning and Teaching Resources

مصادر التعلم والتدريس

	Text	**Available in the Library?**

Required Texts	1. Security in Computing, Fourth Edition, by Charles P. Pfleeger, Pearson Education 2. Cryptography And Network Security Principles And Practice, Fourth or Fifth Edition, William Stallings, Pearso	No
Recommended Texts	Modern Cryptography: Theory and Practice, by Wenbo Mao, Prentice Hall.	No
Websites	https://www.w3schools.com/cpp/cpp_intro.asp	

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.