هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

اعتماد NCAAA
T4 2020

توصيف المقرر الدراسي

اسم المقرر:	Principles of Information Security
رمز المقرر:	DSC511
البرنامج:	Higher Diploma in Cyber Security
الكلية:	Institute of Studies and Consulting Services
المؤسسة:	Majmaah University

المحتويات

أ. التعريف بالمقرر الدراسي:

١. الساعات المعتمدة:
٢. نوع المقرر أ. متطلب جامعة ☐ متطلب كلية ☐ متطلب قسم ☐ أخرى ☐ ب. إجباري ☐ اختياري ☐
٣. السنة / المستوى الذي يقدم فيه المقرر
٤. المتطلبات السابقة لهذا المقرر (إن وجدت)
٥. المتطلبات المتزامنة مع هذا المقرر (إن وجدت)

٦. نمط الدراسة (اختر كل ما ينطبق)

م	نمط الدراسة	عدد الساعات التدريسية	النسبة
1	المحاضرات التقليدية		
2	التعليم المدمج		
3	التعليم الإلكتروني		
4	التعليم عن بعد	44	100%
5	أخرى		

٧. ساعات الاتصال (على مستوى الفصل الدراسي)

م	النشاط	ساعات التعلم
١	محاضرات	44
٢	معمل أو إستوديو	
٣	دروس إضافية	
٤	أخرى (تذكر)	
	الإجمالي	

ب- هدف المقرر ومخرجاته التعليمية:

١. الوصف العام للمقرر:

This course focuses on information security, integrity and privacy techniques. The topics cover the following: Information Security Fundamental, Key Information Security Concepts, Characteristics of Information, and Components of an Information System, Balancing Information Security and Access, Risk Analysis, Security Planning, Physical Security, Security Technology implementation and Information Security Maintenance.

٢. الهدف الرئيس للمقرر

Understand the nature and challenges of information security, the relationship between policy and security, the role of risk management, the mechanisms used to implement policies, the methodologies and technologies for assurance and vulnerability analysis and intrusion detection.

٣. مخرجات التعلم للمقرر:

مخرجات التعلم للمقرر		رمز مخرج التعلم المرتبط للبرنامج
1	المعرفة والفهم	
1.1	State the basic concepts in information security, including security policies, security models, and security mechanisms, risk management, physical security and information security maintenance.	
1.2	Understanding the defenses methods and how to avoid the attack.	
1.3	Understanding the types of attacks.	
1...		
2	المهارات	
2.1	Describe threats to networks, and explain techniques for ensuring network security.	
2.2	Explain the requirements for risk management, and describe how planning and implementing security process.	
2.3	Describe information security maintenance.	
2...		
3	القيم	
3.1		
3.2		
3.3		
3...		

ج. موضوعات المقرر

م	قائمة الموضوعات	ساعات الاتصال
١	Introduction to Information Security	4
٢	The Need for Security	4
٣	Legal, Ethical, and Professional Issues in Information Security	4
٤	Risk Management	4
٥	Planning for Security	6
6	Physical security	6
7	Implementing Information Security	6
8	Security and Personnel	4
9	Information Security Maintenance	6
	المجموع	

د. التدريس والتقييم:

١. ربط مخرجات التعلم للمقرر مع كل من استراتيجيات التدريس وطرق التقييم

الرمز	مخرجات التعلم	استراتيجيات التدريس	طرق التقييم
1.0	المعرفة والفهم		
1.1	State the basic concepts in information security, including security policies, security models, and security	Blackboard Lectures	Discussion, Homeworks, Quiz and Exams

الرمز	مخرجات التعلم	استراتيجيات التدريس	طرق التقييم
	mechanisms, risk management, physical security and information security maintenance.		
1.2	Understanding the defenses methods and how to avoid the attack	Blackboard Lectures	Discussion, Homeworks, Quiz and Exams
…	Understanding the types of attacks	Blackboard Lectures	Discussion, Homeworks, Quiz and Exams
2.0	**المهارات**		
2.1	Describe threats to networks, and explain techniques for ensuring network security.	Blackboard Lectures	Discussion, Homeworks, Quiz and Exams
2.2	Explain the requirements for risk management, and describe how planning and implementing security process.	Blackboard Lectures	Discussion, Homeworks, Quiz and Exams
…	Describe information security maintenance.	Blackboard Lectures	Discussion, Homeworks, Quiz and Exams
3.0	**القيم**		
3.1			
3.2			
…			

٢. أنشطة تقييم الطلبة

م	أنشطة التقييم	توقيت التقييم (بالأسبوع)	النسبة من إجمالي درجة التقييم
١	Midterm Exam	6	30%
٢	Attendance, Discussions and Homeworks	11	30%
٣	Final Exam	12	40%
٤			
٥			
٦			
٧			
٨			

أنشطة التقييم (اختبار تحريري، شفهي، عرض تقديمي، مشروع جماعي، ورقة عمل الخ)

هـ - أنشطة الإرشاد الأكاديمي والدعم الطلابي:

و – مصادر التعلم والمرافق:

١. قائمة مصادر التعلم:

المرجع الرئيس للمقرر	**Principles of Information Security**, By Michael E. Whitman, Herbert J. Mattord Publisher, Cengage Learning; 6th edition (March 13, 2017)
المراجع المساندة	**Fundamentals of Information Systems Security,** by David Kim, Michael G. Solomon Jones & Bartlett Learning; 4th edition (December 24, 2021)
المصادر الإلكترونية	
أخرى	

٢. المرافق والتجهيزات المطلوبة:

العناصر	متطلبات المقرر
المرافق (القاعات الدراسية، المختبرات، قاعات العرض، قاعات المحاكاة ... إلخ)	
التجهيزات التقنية (جهاز عرض البيانات، السبورة الذكية، البرمجيات)	Blackboard Learning System
تجهيزات أخرى (تبعاً لطبيعة التخصص)	

ز. تقويم جودة المقرر:

مجالات التقويم	المقيمون	طرق التقييم

مجالات التقويم (مثل. فاعلية التدريس، فاعلة طرق تقييم الطلاب، مدى تحصيل مخرجات التعلم للمقرر، مصادر التعلم ... إلخ)
المقيمون (الطلبة، أعضاء هيئة التدريس، قيادات البرنامج، المراجع النظير، أخرى (يتم تحديدها)
طرق التقييم (مباشر وغير مباشر)

ح. اعتماد التوصيف

جهة الاعتماد	
رقم الجلسة	
تاريخ الجلسة	

Course specifications

(Postgraduate Degree)

Course Title:	Communication and Network Security
Course Code:	DCS 512
Program:	Diploma in Cybersecurity
College:	Institute of Studies and Consulting Services
Institution:	Majmaah University

Table of Contents

A. Course Identification

1. Credit hours: 4
2. Course type ☒ Required ☐ Elective
3. Level/year at which this course is offered: Level 1
4. Pre-requisites for this course (if any)**:** N/A
5. Co-requisites for this course (if any)**:** N/A

6. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours/Week	Percentage
1	**Traditional classroom**	4	100
2	**Blended**	0	0
3	**E-learning**	0	0
4	**Correspondence**	0	0
5	**Other**	0	0

7. Actual Learning Hours (based on academic semester)

No	Activity	Learning Hours/Week
Contact Hours		
1	**Lecture**	45
2	**Laboratory/Studio**	30
3	**Seminars**	0
4	**Others** (specify)	0
	Total	75
Other Learning Hours*		
1	**Study**	45
2	**Assignments**	30
3	**Library**	0
4	**Projects/Research Essays/Theses**	0
5	**Others** (specify)	0
	Total	75

* The length of time that a learner takes to complete learning activities that lead to achievement of course learning outcomes, such as study time, homework assignments, projects, preparing presentations, library times

B. Course Objectives and Learning Outcomes

1. Course Description

This course aims to introduce wireless networks, including cellular, fixed wireless access, and wireless LANs, secure networking security attacks, network security practice, email security, IP security, web security, intrusion detection and prevention systems. In this course students will also learn advanced concepts in network security and their implementation in network and how to analyze and assess security of network installations in different setups. Hand on experiments include the execution of attacks, the setup of intrusion detection and prevention, securing computers and wired and wireless networks

2. **Course Main Objective:** The rapid growth of mobile telephone use, various satellite services, and now the wireless Internet and wireless LANs are generating tremendous changes in telecommunications and networking. This course aims to introduce secure networking, understanding of the main issues related to security in modern networked systems, also introduce basic and some advanced concepts in security, and their implementation in networks .

3. Course Learning Outcomes

	Course Learning Outcomes (CLOs)	Aligned PLOs*
1	**Knowledge**	
1.1	Understand the design of wireless networks, including cellular, fixed wireless access, and wireless LANs.	K1
1.2	Understand the security issues involved with different Network.	K1
1.3	Understand the Wireless Security Architectures	K1
2	**Skills**	
2.1	Analyze and evaluate a problem as being a possible network security threat.	S1
2.2	Design secure network architectures by using the basic concepts of secure communication.	S2
2.3	Describe security assessment of networks and identify some of the factors driving the need for network security.	S1
3	**Competence**	
3.1		

* Program Learning Outcomes

C. Course Content

No	List of Topics	Contact Hours
1	**Wireless Communication Technology:** Transmission fundamentals, Communication networks, Antennas and propagation, Signal encoding techniques, spread spectrum, Coding and error control.	8
2	**Wireless Networking**: Cellular wireless networks, Mobile IP and WAP	5
3	**Network Security**: The OSI Security Architecture, Security Attacks ,Security Services, Security Mechanisms, Model for Network Security and Standards.	10
4	**Network Access Contro**l: Network Access Control overview, Authentication protocol, IEEE 802. IX Port Based Network Access Control.	10
5	**Network Security Threat Model:** Types of threats, Threats against the application (Cross-site scripting, Session hijacking, Information Disclosure), Threat modeling	8
6	**Wireless Network Security:** Wireless & Mobile Device Security, IEEE 802.11 Wireless LAN, IEEE 802.11i Wireless LAN Security	10
7	**Transport-Level Security:** Secure Socket Layer, Transport Layer Security, HTTPS, Secure Shell SSH)	5
8	**Electronic Mail Security:** Internet mail Architecture, E-mail formats, E-mail threats and security, Pretty Good Privacy, S/MIME, Domain Keys Identified Mail, Domain-based message authentication	8
9	**IP Security:** IP Security Policy Encapsulating security payload Internet Key Exchange Cryptographic Suites	6
10	**Intrusion detection & Firewall:** Intrusion Detection Password Management Firewall Characteristics Types of Firewalls Firewall Basing Firewall Location and Configurations	5
Total		75

D. Teaching and Assessment

1. Alignment of Course Learning Outcomes with Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
1.0	**Knowledge**		
1.1	Understand wireless network architecture, including cellular, fixed wireless access, and wireless LANs.	Classroom Teaching	Test, Lab Based Assignments, Mid Exam, Final Exam
1.3	Understand the security issues involved with different Network.	Classroom Teaching	Test, Lab Based Assignments, Mid Exam, Final Exam
1.4	Understand the Wireless Security Architectures	Classroom Teaching	Test, Lab Based Assignments, Mid Exam, Final Exam
2.0	**Skills**		
2.1	Analyze and evaluate a problem as being a possible network security threat.	Classroom / Lab based Teaching	Test, Lab Based Assignments, Mid Exam, Final Exam
2.2	Design secure network architectures by using the basic concepts of secure communication.	Classroom/ Lab based Teaching	Test, Lab Based Assignments, Mid Exam, Final Exam
2.3	Describe security assessment of networks and identify some of the factors driving the need for network security	Classroom Teaching	Test, Lab Based Assignments, Mid Exam, Final Exam
3.0	**Competence**		
3.1			

2. Assessment Tasks for Students

#	Assessment task*	Week Due	Percentage of Total Assessment Score
1	Assignments	4,7	10%
2	Quizzes	6, 9	5%
3	Written Assessment –Mid Term	8	30%
4	Lab Based Assignment Assessment	10	15%
5	Final Exam	11	40%
	Total		100%

***Assessment task** (i.e., written test, oral test, oral presentation, group project, essay, etc.)

E. Student Academic Counseling and Support

Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice:

Faculty will be assigned students in the corresponding department for academic advising. Students can meet the faculty during advising hours or whenever the faculty is in the office

F. Learning Resources and Facilities

1. Learning Resources

Required Textbooks	Network Security Essentials: Applications and Standards (6th Edition) by William Stallings ISBN-13: 978-0134527338 Pearson (Aug 7, 2016)
Essential Reference Materials	1. Introduction to Network Security by Douglas Jacobson Chapman & Hall/CRC Computer and Information Science Series ISBN-13: 978-1584885436 2. Introduction to Network Security: Theory and Practice 2nd Edition by Jie Wang , Zachary A. Kissel Publisher: Wiley; 2 edition (October 5, 2015) ISBN-13: 978-1118939482 3. Wireless Communication and Networks By Williant Stallings, Pearson new International Ed.(Per05),2013
Electronic Materials	
Other Learning Materials	

2. Educational and research Facilities and Equipment Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	Classroom and Network Lab
Technology Resources (AV, data show, Smart Board, software, etc.)	PC or Laptop with Windows/Linux, Smart Board, Projector
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	Network Lab (Available)

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
	Course instructor	Direct

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Assignment/Quiz/Mid Term/ Final Exam assessment (Extent of achievement of course learning outcomes)		
Course Survey in the middle of the semester and at the end of the semester(Effectiveness of teaching and assessment)	Students	Indirect
Extent of achievement of course learning outcomes	Students	Indirect
Final Exam Answer Scripts Verification	Peer faculty members	Review (Direct)

Evaluation Areas/Issues (e.g., Effectiveness of teaching and assessment, Extent of achievement of course learning outcomes, Quality of learning resources, etc.)
Evaluators (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)
Assessment Methods (Direct, Indirect)

H. Specification Approval Data

Council / Committee	
Reference No.	
Date	

هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

اعتماد NCAAA
T4 2020

توصيف المقرر الدراسي

اسم المقرر:	أمن نظم التشغيل
رمز المقرر:	DSC 513
البرنامج:	الأمن السيبراني
الكلية:	معهد الدراسات والخدمات الاستشارية
المؤسسة:	جامعة المجمعة

المحتويات

أ. التعريف بالمقرر الدراسي:

١. الساعات المعتمدة: ٤ ساعات معتمدة

٢. نوع المقرر

أ. متطلب جامعة ☐ متطلب كلية ☐ متطلب قسم ☑ أخرى ☐

ب. إجباري ☑ اختياري ☐

٣. السنة / المستوى الذي يقدم فيه المقرر:
الأولى / المستوى الأول

٤. المتطلبات السابقة لهذا المقرر (إن وجدت)
لا يوجد

٥. المتطلبات المتزامنة مع هذا المقرر (إن وجدت)
لا يوجد

٦. نمط الدراسة (اختر كل ما ينطبق)

م	نمط الدراسة	عدد الساعات التدريسية	النسبة
1	المحاضرات التقليدية	٢٢	%٥٠
2	التعليم المدمج	-	-
3	التعليم الإلكتروني	٢٢	%٥٠
4	التعليم عن بعد	-	-
5	أخرى	-	-

٧. ساعات الاتصال (على مستوى الفصل الدراسي)

م	النشاط	ساعات التعلم
١	محاضرات	٤٤
٢	معمل أو إستوديو	-
٣	دروس إضافية	-
٤	أخرى (تذكر)	-
	الإجمالي	٤٤

ب- هدف المقرر ومخرجاته التعليمية:

١. الوصف العام للمقرر:

يهتم مقرر أمن أنظمة التشغيل بدراسة وفهم أنظمة تشغيل الحاسب – والتي تعد أحد أهم البرمجيات في جهاز الحاسب الآلي والمشغل الرئيس له – من حيث تعريفها وتركيبها وكيفية عملها مع البرمجيات والمعدات في منظومة الحاسب، وكذلك التطرق إلى فهم ومعرفة أنواع وأشكال التهديدات الأمنية التي يتعرض لها وسبل تأمينه ضدها وتوفير الحماية اللازمة لصدها وتفاديها.

٢. الهدف الرئيس للمقرر

يهدف هذا المقرر إلى تعريف الطالب بمفهوم أنظمة تشغيل الحاسب الآلي ووظائفها وكيفية تفاعلها وإدارتها لمكونات الحاسب الآلي، إلى جانب التعرف على أنواع التهديدات الأمنية التي تتعرض لها نظم التشغيل واستراتيجيات تأمينها واستخدام أنظمة وأدوات الفحص والحماية المناسبة لصد الهجمات والتهديدات والوقاية منها.

٣. مخرجات التعلم للمقرر:

	مخرجات التعلم للمقرر	رمز مخرج التعلم المرتبط للبرنامج
1	**المعرفة والفهم**	
1.1	التعرف على أنظمة التشغيل وأهميتها ووظائفها وأنواعها	
1.2	التعرف على كيفية إدارة وتفاعل أنظمة التشغيل مع المعدات والبرمجيات	
1.3	التعرف على التهديدات والمخاطر الأمنية على أنظمة التشغيل وسبل الحماية والوقاية منها	
2	**المهارات**	
2.1	تمييز أنواع نظم التشغيل وتطبيقاتها المتنوعة	
2.2	تحليل أنواع التهديدات والمخاطر الأمنية على نظم التشغيل	
2.3	محاكاة تثبيت واستخدام أنظمة التشغيل المتنوعة	
2.4	تطبيق أدوات فحص وتحليل المخاطر واستخدام برمجيات الحماية	
3	**القيم**	
3.1	العمل في بيئة المجموعات	
3.2	استغلال وتنظيم الوقت	
3.3	تعزيز الأمانة العلمية	

ج. موضوعات المقرر

م	قائمة الموضوعات	ساعات الاتصال
١	التعريف بأنظمة التشغيل وأهميتها ووظائفها	٤
٢	تفاعل أنظمة التشغيل مع البرمجيات والمعدات في نظام الحاسب	٤
٣	إدارة نظم التشغيل للعمليات والذاكرة ووحدات التخزين	٤
٤	أنواع أنظمة التشغيل	٤
٥	التهديدات والمخاطر الأمنية على أنظمة التشغيل	٦
٦	استراتيجيات الأمان والحماية لأنظمة التشغيل	٨
٧	تثبيت والتعامل مع أنظمة التشغيل (Windows , Linux) باستخدام VirtualBox	٨
٨	التعامل مع أدوات فحص وتحليل المخاطر واستخدام برمجيات الحماية	٦
	المجموع	٤٤

د. التدريس والتقييم:

١. ربط مخرجات التعلم للمقرر مع كل من استراتيجيات التدريس وطرق التقييم

الرمز	مخرجات التعلم	استراتيجيات التدريس	طرق التقييم
1.0	**المعرفة والفهم**		
1.1	التعرف على أنظمة التشغيل وأهميتها ووظائفها وأنواعها	- التدريس المباشر ○ المحاضرات ○ شرائح العروض التقديمية ○ المناقشات الفصلية	- الواجبات والتكليفات المنزلية. - الاختبارات القصيرة - الاختبار الفصلي - الاختبار النهائي
1.2	التعرف على كيفية إدارة وتفاعل أنظمة التشغيل مع المعدات والبرمجيات		
1.3	التعرف على التهديدات والمخاطر الأمنية على أنظمة التشغيل وسبل الحماية والوقاية منها	- التدريس غير المباشر ○ من خلال الأسئلة الاستطلاعية والاستكشافية	- البحث عبر في الكتب وعبر الانترنت

الرمز	مخرجات التعلم	استراتيجيات التدريس	طرق التقييم
2.0	**المهارات**		
2.1	تمييز أنواع نظم التشغيل وتطبيقاتها المتنوعة	- التدريس المباشر ○ المحاضرات ○ شرائح العروض التقديمية ○ المناقشات الفصلية ○ التطبيق العملي - التدريس غير المباشر ○ من خلال الأسئلة الاستطلاعية والاستكشافية	- الواجبات المنزلية - الاختبارات القصيرة - التكليفات أثناء التطبيق العملي
2.2	تحليل أنواع التهديدات والمخاطر الأمنية على نظم التشغيل		
2.3	محاكاة تثبيت واستخدام أنظمة التشغيل المتنوعة		
2.4	تطبيق أدوات فحص وتحليل المخاطر واستخدام برمجيات الحماية		
3.0	**القيم**		
3.1	العمل في بيئة المجموعات	- حث الطلاب على العمل والتعاون معاً في مجموعات منظمة المهام. - حث الطلاب على بذل الجهد الفردي مهما كان مستواه، وإثابتهم على ذلك.	- متابعة الطلاب أثناء التطبيق العملي - متابعة الطلاب أثناء المناقشات والمشاركة أثناء المحاضرة - مراجعة أداء الواجبات والتكليفات - مراجعة نتائج الاختبارين الفصلي والنهائي
3.2	استغلال وتنظيم الوقت		
3.3	تعزيز الأمانة العلمية		

٢. أنشطة تقييم الطلبة

م	أنشطة التقييم	توقيت التقييم (بالأسبوع)	النسبة من إجمالي درجة التقييم
١	**اختبار منتصف الفصل الدراسي**	٩	%٣٠
٢	**الواجبات والتكاليف**	١٠،٨،٦،٣	%٢٠
٣	**الاختبارات القصيرة**	٧ ، ٤	%١٠
٤	**الاختبار النهائي**	١٢	%٤٠

أنشطة التقييم (اختبار تحريري، شفهي، عرض تقديمي، مشروع جماعي، ورقة عمل الخ)

هـ - أنشطة الإرشاد الأكاديمي والدعم الطلابي:

- **تحديد ساعة مكتبية واحدة يومياً.**
- **تقديم المساعدة للطلبة الذين لديهم ضعف في التقييم والتفاعل الفصلي من خلال عقد لقاءات معهم لحل مشكلاتهم وإعطاءهم نصائح وإرشادات أكاديمية.**
- **تحفيز الطلبة على التفاعل والمشاركة الفصلية.**

و – مصادر التعلم والمرافق:

١. قائمة مصادر التعلم:

المرجع الرئيس للمقرر	- ***Operating System Security, Trent Jaeger, Morgan and Claypool Publishers, 2008.*** - ***Operating System Concepts, Avi Silberschatz - Peter Baer Galvin & Greg Gagne,10th Edition, John Wiley & Sons, Inc., 2018.***
المراجع المساندة	- ***Network Security Essentials (Applications & Standards), William Stallings, 6th edition, Pearson, 2017*** - ***Essential Checkpoints Firewall-1: An Installation, Configuration, and Troubleshooting Guide, by Dameon D. Welch-Abernathy, January 15, 2002, Addison-Wesley Pub. Co.; ISBN: 0201699508*** - ***Hacking Exposed, by Joel Scambray, Stuart McClure, George Kurtz, McGraw-Hill Proffesional Pub.; October 11, 2000, ISBN:0072127481.***
المصادر الإلكترونية	- https://www.youtube.com/watch?v=Xu9B7Wnutw0&list=PLGN_yckFx1civO91pjR7imIcnAiG3CR4l&index=1 - https://www.youtube.com/watch?v=fAhvVqw_dus
أخرى	

٢. المرافق والتجهيزات المطلوبة:

العناصر	متطلبات المقرر
المرافق (القاعات الدراسية، المختبرات، قاعات العرض، قاعات المحاكاة ... إلخ)	قاعة صفية (فصلية) مجهزة بالآتي: - جهاز حاسب آلي مكتبي - سبورة عادية - بروجكتور رقمي - البرمجيات الآتية يجب أن تكون مثبتة أو متوفرة كصور (Images) على جهاز الحاسب – بأحدث الإصدارات –: ○ **MS Windows** ○ **MS Office** ○ **Kaspersky Internet Security** ○ **Zone Alarm Firewall** ○ **Kali Linux** ○ **Cisco Packet Tracer** ○ **Oracle VirtualBox** - اتصال عالي السرعة بشبكة الانترنت

العناصر	متطلبات المقرر
التجهيزات التقنية (جهاز عرض البيانات، السبورة الذكية، البرمجيات)	معمل حاسب آلي يضم التجهيزات الآتية: - ٣٠ أجهزة حاسب آلي - بروجكتور رقمي - سبورة كتابة عادية - سبورة ذكية - البرمجيات الآتية يجب أن تكون مثبتة أو متوفرة كصور (Images) على جهاز الحاسب – بأحدث الإصدارات –: ○ **MS Windows** ○ **MS Office** ○ **Kaspersky Internet Security** ○ **Zone Alarm Firewall** ○ **Kali Linux** ○ **Cisco Packet Tracer** ○ **Oracle VirtualBox** - اتصال عالي السرعة بشبكة الانترنت
تجهيزات أخرى (تبعاً لطبيعة التخصص)	- **طابعة ليزر مشتركة في معمل الحاسب** - **ماسح ضوئي مشترك في معمل الحاسب** - **سماعات صوتية**

ز. تقويم جودة المقرر:

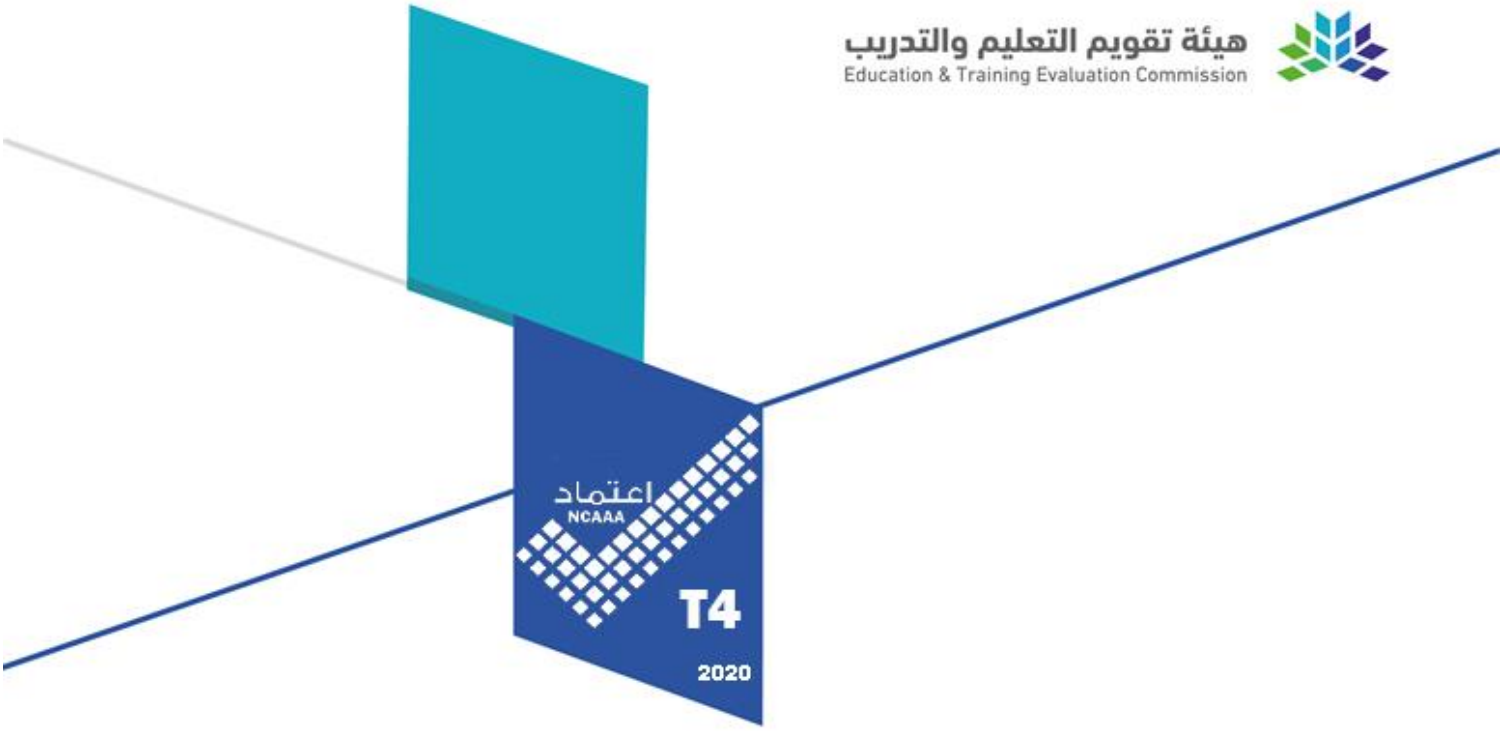
مجالات التقويم	المقيمون	طرق التقييم
فاعلية التدريس	**قيادات البرنامج، أعضاء هيئة التدريس، المراجع النظير، الطلبة**	**مباشر**
فاعلية طرق تقييم الطلاب	**أعضاء هيئة التدريس، المراجع النظير الطلبة**	**مباشر** **غير مباشر**
مدى تحصيل مخرجات التعلم للمقرر	**قيادات البرنامج، أعضاء هيئة التدريس المراجع النظير**	**مباشر** **غير مباشر**
فاعلية مصادر التعلم	**الطلبة، أعضاء هيئة التدريس، المراجع النظير**	**مباشر**

مجالات التقويم (مثل. فاعلية التدريس، فاعلة طرق تقييم الطلاب، مدى تحصيل مخرجات التعلم للمقرر، مصادر التعلم ... إلخ)
المقيمون (الطلبة، أعضاء هيئة التدريس، قيادات البرنامج، المراجع النظير، أخرى (يتم تحديدها)
طرق التقييم (مباشر وغير مباشر)

ح. اعتماد التوصيف

جهة الاعتماد	
رقم الجلسة	
تاريخ الجلسة	

هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission



Course Specifications

Course Title:	Cryptography Fundamentals
Course Code:	DCS 514
Program:	Diploma in Cybersecurity
Department:	Information Technology
College:	Institute of Studies and Consulting Services
Institution:	Majmaah University

Table of Contents

A. Course Identification

1. Credit hours: 4
2. Course type **a.** University ☐ College ☐ Department ☐ Others ☐ **b.** Required ☑ Elective ☐
3. Level/year at which this course is offered: 2
4. Pre-requisites for this course (if any)**:**
5. Co-requisites for this course (if any)**:**

6. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	**Traditional classroom**	2	50
2	**Blended**		
3	**E-learning**		
4	**Distance learning**	2	50
5	**Other**		

7. Contact Hours (based on academic semester)

No	Activity	Contact Hours
1	**Lecture**	36
2	**Laboratory/Studio**	12
3	**Tutorial**	
4	**Others** (specify)	
	Total	48

B. Course Objectives and Learning Outcomes

1. Course Description

This course helps the students to learn cryptographic concepts. In this course students will learn the workings of cryptographic systems and use them in real-world applications. Topics covered include cryptographic primitives such as symmetric encryption, Number Theory, public key encryption, hashing functions, digital signatures, and message authentication codes, cryptographic protocols, key establishment, and Electronic commerce.

2. Course Main Objective

This course provides students with a thorough review of cryptography and cryptographic techniques as they apply to the area of cyber and computer security.

3. Course Learning Outcomes

CLOs		Aligned PLOs
1	**Knowledge and Understanding**	
1.1	Understand the concept of cryptographic algorithms.	K1
1.2	Study different cryptography techniques along with their advantages and disadvantages.	K1
1.3	Understand Digital signatures in practice with legal/regulatory aspects.	K1
1.4	Learn the current state of the art techniques that are employed for defeating secure systems.	K1
2	**Skills :**	
2.1	Apply the current state of the art techniques that are employed for defeating secure systems.	S1
2.2	Analyze RSA The RSA and Diffie–Hellman Key Exchange Algorithms	S1
2.3	Analyze hashing functions, message authentication codes and key establishment	S1
2...		
3	**Values:**	
3.1		
3.2		
3.3		
3...		

C. Course Content

No	List of Topics	Contact Hours
1	**Introduction to Cryptography:** Why Cryptography, Security Attacks, Symmetric and Asymmetric Cryptography, Plain text, Cipher text, encryption and decryption.	8
2	**Mathematics of Cryptography:** GCD, Modular Inverse , Multiplicative Inverse, Euclidean Algorithm, Extended Euclidean Algorithm, Euler's Phi Function and Fermat's Little Theorem and Euler's Theorem	4
3	**Traditional Symmetric Key Ciphers and Classical Cryptography:** Substitution Cipher (Caesar Cipher, Mono alphabetic Cipher, Play fair Cipher) and Transposition Cipher (Rail Fence cipher, Columnar Transposition, Double Transposition Cipher)	10
4	**Modern Symmetric-Key Cipher**: Stream cipher, Block cipher, Data Encryption Standard (DES), Triple DES, AES (Advanced Encryption Standard)	8
5	**Asymmetric Key Cryptography**: The RSA Cryptosystem, Diffie–Hellman Key Exchange,	6
6	**Cryptographic Hash Functions:** Security Requirements of Hash Functions, Secure Hash Algorithm	4
7	**Digital Signatures:** The RSA Signature Scheme, The Digital Signature Algorithm (DSA), standard methods of encoding of digital signatures and certificates (X.509) in Electronic commerce	4
8	**Revision**	4
Total		48

D. Teaching and Assessment

1. Alignment of Course Learning Outcomes with Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
1.0	**Knowledge and Understanding**		
1.1	Understand the concept of cryptographic algorithms.	Classroom Teaching	Test, Lab Based Assignments, Mid Exam, Final Exam
1.2	Study different cryptography techniques along with their advantages and disadvantages.	Classroom Teaching	Test, Lab Based Assignments, Mid Exam, Final Exam
1.3	Understand Digital signatures in practice with legal/regulatory aspects.	Classroom Teaching	Test, Lab Based Assignments, Mid Exam, Final Exam
1.4	Learn the current state of the art techniques that are employed for defeating secure systems.	Classroom Teaching	Test, Lab Based Assignments, Mid Exam, Final Exam
2.0	**Skills**		
2.1	Apply the current state of the art techniques that are employed for defeating secure systems.	Classroom / Lab based Teaching	Test, Lab Based Assignments, Mid Exam, Final Exam
2.2	Analyze RSA The RSA and Diffie–Hellman Key Exchange Algorithms	Classroom/ Lab based Teaching	Test, Lab Based Assignments, Mid Exam, Final Exam
2.2	Analyze hashing functions, message authentication codes and key establishment	Classroom /Lab based Teaching	Test, Lab Based Assignments, Mid Exam, Final Exam
3.0	**Values**		
3.1			
3.2			
…			

2. Assessment Tasks for Students

#	Assessment task*	Week Due	Percentage of Total Assessment Score
1	Assignment I/II	5, 10	20%
2	Quizzes I	8	10%
3	Written Assessment –Mid Term	7	30%
4	Final Exam	12	40%
	Total		100%

***Assessment task** (i.e., written test, oral test, oral presentation, group project, essay, etc.)

E. Student Academic Counseling and Support

Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice :

Faculty will be assigned students in the corresponding department for academic advising. Students can meet the faculty during advising hours or whenever the faculty is in the office.

F. Learning Resources and Facilities

1.Learning Resources

Required Textbooks	Paar, Christof, and Jan Pelzl. Understanding Cryptography: A Textbook for Students and Practitioners. Springer Science & Business Media, 2009
Essential References Materials	1. CRYPTOGRAPHY AND NETWORK SECURITY (7th Edition) by William Stallings , 2018. 2. Lindell, Yehuda, and Jonathan Katz. *Introduction to modern cryptography*. Chapman and Hall/CRC, 2014. ISBN-13: 978-1466570269 3. Smart Cards, Tokens, Security and Applications by Keith E. Mayes and Konstantinos Markantonakis. ISBN-13: 978-0-387-72197-2 e-ISBN-13: 978-0-387-72198-9, 2017 Springer Science 4. W. Stallings, "Cryptography and network security: principles and practice" Pearson; 2017. ISBN-13: 978-0134444284
Electronic Materials	
Other Learning Materials	

2. Facilities Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	Classroom and a Lab
Technology Resources (AV, data show, Smart Board, software, etc.)	PC or Laptop with Windows/Linux, Smart Board, Projector
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	Network and DF Lab (Available)

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Assignment/Quiz/Mid Term/ Final Exam assessment (Extent of achievement of course learning outcomes)	Course instructor	Direct
Course Survey in the middle of the semester and at the end	Students	Indirect

Evaluation Areas/Issues	Evaluators	Evaluation Methods
of the semester (Effectiveness of teaching and assessment)		
Extent of achievement of course learning outcomes	Students	Indirect
Final Exam Answer Scripts Verification	Peer faculty members	Review (Direct)

Evaluation areas (e.g., Effectiveness of teaching and assessment, Extent of achievement of course learning outcomes, Quality of learning resources, etc.)
Evaluators (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)
Assessment Methods (Direct, Indirect)

H. Specification Approval Data

Council / Committee	
Reference No.	
Date	

هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

اعتماد NCAAA T4 2020

Course Specifications

Course Title:	**Information Security Management**
Course Code:	**DCS521**
Program:	**Higher Diploma in Cyber Security**
Department:	
College:	
Institution:	**Majmaah University**

Table of Contents

A. Course Identification

1. Credit hours: 4
2. Course type **a.** University ☐ College ☐ Department ☐ Others ☐ **b.** Required ☐ Elective ☐
3. Level/year at which this course is offered:
4. Pre-requisites for this course (if any)**:**
5. Co-requisites for this course (if any)**:**

6. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	**Traditional classroom**		
2	**Blended**		
3	**E-learning**	44	100%
4	**Distance learning**		
5	**Other**		

7. Contact Hours (based on academic semester)

No	Activity	Contact Hours
1	**Lecture**	44
2	**Laboratory/Studio**	
3	**Tutorial**	
4	**Others** (specify)	
	Total	

B. Course Objectives and Learning Outcomes

1. Course Description

This course is intended to give students an introduction to a variety of information and cyber security topics. As an introductory course, it will cover foundational technical concepts as well as managerial and policy topics. The purpose of the course lectures, assignments, reading, in-class presentations, and examinations are to ensure students have sufficient technical awareness and managerial competence that will enable them to pursue advanced study in information security policy and management as they progress through their program. There is no prerequisite for this course, however successful students will have fundamental knowledge of information and computer systems, and a general awareness of security issues in these systems.

2. Course Main Objective

This course investigates the whole process of information security management and associated activities including the concepts used and practices prescribed by relevant standards, such as those defined by ISO/IEC. A holistic view of information security management is taken,

including risk management, the formulation of security policies, business continuity and resilience. Selected socio-technical topics that are important for information security management will also be covered. These shall include AAA (authentication, authorization and accountability), important legal aspects especially data protection and privacy laws, data protection impact assessment, usability analysis and management, wider human factors in cyber security such as social engineering attacks and the importance of a positive cyber security culture for encouraging secure behaviors of employees and users.

3. Course Learning Outcomes

CLOs		Aligned PLOs
1	**Knowledge and Understanding**	
1.1	The candidate possess through knowledge of the fundamental theories, models practices of information security management for both large and small organizations.	K1
1.2	The candidate possess insight and understanding of ethical and legal aspect information security management and privacy management.	K1
1.3	The candidate possesses good understanding of the risk management processes.	K1
1.4	The candidate possesses good understanding of security planning and incident management process.	K2
1.5	The candidate possess insight of the technological innovation process in IT security and its effect on security management.	K2
1.6	The candidate possess basic knowledge of the standards in information security management.	K2
2	**Skills :**	
2.1	The candidate is capable of analyzing existing theory, models and methods in the field of information security management and work independently on solving theoretical and practical problems.	S1
2.2	The candidate is capable of applying his/her knowledge to both modeling the potential problems and the solutions in information security management and be able to communicate this problems and solutions using basic theoretical skills.	S2
2.3	The candidate is capable of using and the basic terminology and is aware of the basic standards used in the area of information security management.	S3
2...		
3	**Values:**	
3.1	Can participate in group work and manage different organization roles of information security management.	
3.2		
3.3		
3...		

C. Course Content

No	List of Topics	Contact Hours
1	Introduction to Information Security Management	4
2	Planning for Security	4
3	Planning for Contingencies	4

4	Information Security Policy	4
5	Developing the Security Program	4
6	Security Management Models and Practices	4
7	Risk Management	4
8	Protection Mechanism	4
9	Personnel and Security	4
10	Law and Ethics	4
11	Information Security Project Management	4
Total		

D. Teaching and Assessment

1. Alignment of Course Learning Outcomes with Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
1.0	**Knowledge and Understanding**		
1.1	The candidate possess through knowledge of the fundamental theories, models practices of information security management for both large and small organizations.	Blackboard Lectures	Discussion, Homeworks, Quiz and Exams
1.2	The candidate possess insight and understanding of ethical and legal aspect information security management and privacy management.	Blackboard Lectures	Discussion, Homeworks, Quiz and Exams
1.3	The candidate possesses good understanding of the risk management processes.	Blackboard Lectures	Discussion, Homeworks, Quiz and Exams
1.4	The candidate possesses good understanding of security planning and incident management process.	Blackboard Lectures	Discussion, Homeworks, Quiz and Exams
1.5	The candidate possess insight of the technological innovation process in IT security and its effect on security management.	Blackboard Lectures	Discussion, Homeworks, Quiz and Exams
1.6	The candidate possess basic knowledge of the standards in information security management.	Blackboard Lectures	Discussion, Homeworks, Quiz and Exams
2.0	**Skills**		
2.1	The candidate is capable of analyzing existing theory, models and methods in the field of information security management and work independently on solving theoretical and practical problems.	Blackboard Lectures	Discussion, Homeworks, Quiz and Exams
2.2	The candidate is capable of applying his/her knowledge to both modeling the potential problems and the solutions in information security	Blackboard Lectures	Discussion, Homeworks, Quiz and Exams

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
	management and be able to communicate this problems and solutions using basic theoretical skills.		
2.3	The candidate is capable of using and the basic terminology and is aware of the basic standards used in the area of information security management.	Blackboard Lectures	Discussion, Homeworks, Quiz and Exams
3.0	**Values**		
3.1	Can participate in group work and manage different organization roles of information security management.	Encourage the students to work and collaborate together in groups of organized tasks.	- Encouraging students to make individual efforts, whatever their level, and rewarding them for that. - Follow-up of students during practical application - Follow-up students during discussions and participation during the lecture - Reviewing the performance of duties and assignments
3.2			
…			

2. Assessment Tasks for Students

#	Assessment task*	Week Due	Percentage of Total Assessment Score
1	Midterm Exam	6	30%
2	Attendance, Discussions and Homeworks	٣،5،٨،10	30%
3	Final Exam	12	40%
4			
5			
6			
7			
8			

***Assessment task** (i.e., written test, oral test, oral presentation, group project, essay, etc.)

E. Student Academic Counseling and Support

Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice:

Faculty will be assigned students in the corresponding department for academic advising. Students can meet the faculty during advising hours or whenever the faculty is in the office

F. Learning Resources and Facilities

1.Learning Resources

Required Textbooks	**Information Security Management,** 2nd Edition by Michael Workman , ISBN-10: 1284211657, ISBN-13: 978-1284211658, Jones & Bartlett Learning, November 12, 2021.
Essential References Materials	
Electronic Materials	
Other Learning Materials	

2. Facilities Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	
Technology Resources (AV, data show, Smart Board, software, etc.)	Blackboard Learning System
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods

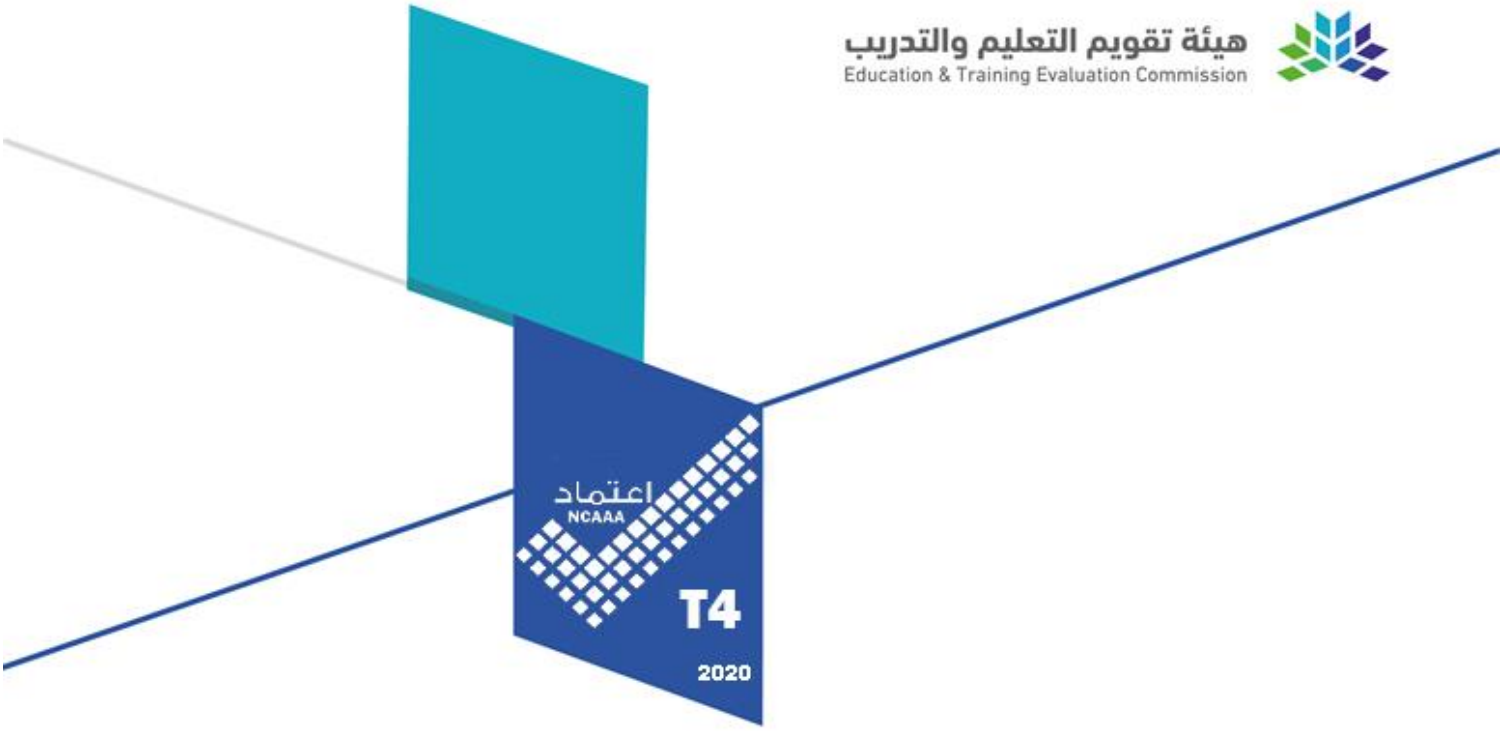
Evaluation areas (e.g., Effectiveness of teaching and assessment, Extent of achievement of course learning outcomes, Quality of learning resources, etc.)
Evaluators (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)
Assessment Methods (Direct, Indirect)

H. Specification Approval Data

Council / Committee	
Reference No.	

Date	

هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission



Course Specifications

Course Title:	Secure Software Development
Course Code:	DSC 522
Program:	Diploma in Cybersecurity
Department:	Information Technology
College:	Institute of Studies and Consulting Services
Institution:	Majmaah University

Table of Contents

A. Course Identification

1. Credit hours: 4
2. Course type **a.** University ☐ College ☐ Department ☐ Others ☐ **b.** Required ☑ Elective ☐
3. Level/year at which this course is offered: 2
4. Pre-requisites for this course (if any)**:** N/A
5. Co-requisites for this course (if any)**:** N/A

6. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	**Traditional classroom**	2	50
2	**Blended**		
3	**E-learning**		
4	**Distance learning**	2	50
5	**Other**		

7. Contact Hours (based on academic semester)

No	Activity	Contact Hours
1	**Lecture**	36
2	**Laboratory/Studio**	12
3	**Tutorial**	
4	**Others** (specify)	
	Total	48

B. Course Objectives and Learning Outcomes

1. Course Description

This course will provide students to understand the theories and tools used for secure software design, threat analysis, secure coding, and vulnerability analysis. Students will study, in-depth, vulnerability classes to understand how to protect software and how to develop secure software. This course will also cover various analysis and design techniques for improving software security.

2. Course Main Objective

- Understand the theories and tools used for secure software design, threat analysis, secure coding, and vulnerability analysis
- Analyze secure software design and post-implementation security success factors, deliverables, and metrics
- Identify the nature and challenges of Software Security
- Understand the relationship between policy and security
- Apply various methodologies and technologies for Software Assurance

3. Course Learning Outcomes

CLOs		Aligned PLOs
1	**Knowledge and Understanding**	
1.1	Recognize the risks, threats, and vulnerabilities associated with the transformed digital world.	K1
1.2	Understand how to protect software and how to develop secure software.	K1
2	**Skills :**	
2.1	Analyze issues in Web applications Security and technologies	S1
2.2	Apply code auditing practices, and analyze vulnerabilities in memory management.	S1
2.3	Evaluate the optimal design techniques for improving software security.	S2
3	**Values:**	
3.1	Works within a team and takes responsibility	V1
3.2		
3.3		
3...		

C. Course Content

No	List of Topics	Contact Hours
1	**Introduction to software security** Discussion of the risks, threats, and vulnerabilities associated with the transformation to a digital world, including a look at how business, government, and individuals operate today	10
2	**software development methods** Waterfall, Iterative, Spiral, Agile	5
3	**Functional vs Non Functional software Requirements** Approaches to NFRs, Non-Functional Testing, Families of NFRs	6
4	**Secure Design Considerations** client–server applications, Analyzing vulnerabilities related to memory management, data types, and malformed data, Identifying a Web Application's Attack Surface, Analyze Web applications Security and technologies, use Ubuntu OS to secure software concepts	8
5	**Dynamic application security testing** Penetration Testing, software development using testing and for runtime tools security, DAST, IAST, and RASP testing methodologies	5
6	**Open SAMM framework** Study the most recent updates in Information Systems Security laws, certificates, standards, amendments, and the proposed Federal Information Security Amendments	6
7	**The impact of emerging technology on software security** effect of machine learning and artificial intelligence on secure software development	4
8	**Review**	4
Total		48

D. Teaching and Assessment

1. Alignment of Course Learning Outcomes with Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
1.0	**Knowledge and Understanding**		
1.1	Describe the risks, threats, and vulnerabilities associated with the transformed digital world.	Classroom Teaching	Class Test, Mid Exam, Final Exam
1.2	Understand how to protect software and how to develop secure software.	Classroom Teaching	Class Test, Mid Exam, Final Exam
2.0	**Skills**		
2.1	Analyze issues in Web applications Security and technologies	Classroom Teaching/ Lab based Teaching	Group Assignment Mini Project
2.2	Apply code auditing practices, and analyze vulnerabilities in memory management.	Classroom Teaching/ Lab based Teaching	Group Assignment Mini Project
2.3	Evaluate the optimal design techniques for improving software security.	Classroom Teaching/ Lab based Teaching	Group Assignment Mini Project
3.0	**Values**		
3.1	Works within a team and takes responsibility	-Encourage the Students to work and collaborate together in groups of organized tasks. -Encouraging students to make individual efforts, whatever their level, and rewarding them for that.	- Follow-up students during discussions and participation during the lecture -Reviewing the performance of duties and assignments -Review the results of the semester and final exams
3.2			
…			

2. Assessment Tasks for Students

#	Assessment task*	Week Due	Percentage of Total Assessment Score
1	Assignment I/II	5-10	20%
2	Case Study / Presentations	8	10%
3	Written Assessment –Mid Term	7	30%
4	Final Exam	12	40%
	Total		100%

***Assessment task** (i.e., written test, oral test, oral presentation, group project, essay, etc.)

E. Student Academic Counseling and Support

Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice :

There will be an academic advisory committee for guidance and counselling

F. Learning Resources and Facilities

1.Learning Resources

Required Textbooks	Cyber Security Engineering: A Practical Approach for Systems and Software Assurance (SEI Series in Software Engineering) 1st Edition , Nancy R. Mead and Carol Woody, Addison-Wesley Professional, 2017.
Essential References Materials	1. Principles of Computer Security, Fourth Edition, Wm. Arthur Conklin and at el., McGraw-Hill Education, 2015 2. Computer Security: Art and Science (2 Volume Set) 1st Edition, Matt Bishop, Addison-Wesley Professional, 2015 3. Core Software Security: Security at the Source 1st Edition, James Ransome and Anmol Misra, Auerbach Publications, 2013. Fundamentals of Information Systems Security, 2nd Edition, David Kim and Michael G. Solomon, Jones & Bartlett Learning, 2014.
Electronic Materials	
Other Learning Materials	

2. Facilities Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	Classroom and a Lab
Technology Resources (AV, data show, Smart Board, software, etc.)	PC or Laptop with Windows/Linux, Smart Board, Projector
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	Network and DF Lab (Available)

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Test/Quiz/Mid Term/ Final Exam assessment (Extent of achievement of course learning outcomes)	Course instructor	Direct

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Course Survey in the middle of the semester and at the end of the semester (Effectiveness of teaching and assessment)	Students	Indirect
Extent of achievement of course learning outcomes	Students	Indirect
Final Exam Answer Scripts Verification	Peer faculty members	Review (Direct)

Evaluation areas (e.g., Effectiveness of teaching and assessment, Extent of achievement of course learning outcomes, Quality of learning resources, etc.)
Evaluators (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)
Assessment Methods (Direct, Indirect)

H. Specification Approval Data

Council / Committee	
Reference No.	
Date	

Course specifications

(Postgraduate Degree)

Course Title:	Ethical Hacking
Course Code:	DCS 523
Program:	Diploma in Cybersecurity
Department:	Information Technology
College:	College of Computer and Information Sciences
Institution:	Majmaah University

Table of Contents

A. Course Identification

1. Credit hours: 4
2. Course type ☒ Required ☐ Elective
3. Level/year at which this course is offered: Level 2
4. Pre-requisites for this course (if any)**:** N/A
5. Co-requisites for this course (if any)**:** N/A

6. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	**Traditional classroom**	5	100
2	**Blended**	0	0
3	**E-learning**	0	0
4	**Correspondence**	0	0
5	**Other**	0	0

7. Actual Learning Hours (based on academic semester)

No	Activity	Learning Hours
Contact Hours		
1	**Lecture**	45
2	**Laboratory/Studio**	30
3	**Seminars**	0
4	**Others** (specify)	0
	Total	75
Other Learning Hours*		
1	**Study**	60
2	**Assignments**	0
3	**Library**	0
4	**Projects/Research Essays/Theses**	0
5	**Others** (specify)	0
	Total	60

* The length of time that a learner takes to complete learning activities that lead to achievement of course learning outcomes, such as study time, homework assignments, projects, preparing presentations, library times

B. Course Objectives and Learning Outcomes

1. Course Description

This course aims to provide the students the knowledge of ethical hacking techniques commonly used to breech and exploit corporate networks and to identify how and when they are used. This course teaches penetration-testing techniques that quickly, efficiently and most importantly methodically uncover vulnerabilities in operating systems, applications and networks. Students will learn core skills and techniques that every penetration tester needs.

2. Course Main Objective

This course gives knowledge of various ethical hacking and penetration techniques and the practical skills required to perform penetration testing.

3. Course Learning Outcomes

Course Learning Outcomes (CLOs)		Aligned PLOs*
1	**Knowledge**	
1.1	Understand the basics of ethical hacking.	K1
1.2	Know the legal implications of ethical hacking.	K1
2	**Skills**	
2.1	Apply the penetration testing techniques to uncover vulnerabilities in operating systems, applications and networks.	S1
3	**Competence**	
3.1	Implement effective countermeasures to defend attacks on operating system and networks based on team engaged work.	C1

* Program Learning Outcomes

Program Learning Outcomes:

K1: Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions

K2: Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles

C1: Identify and analyze user needs and to take them into account in the selection, creation, integration, evaluation, and administration of computing-based systems

C. Course Content

No	List of Topics	Contact Hours
1	Introduction to Ethical Hacking	5
2	Network Penetration Testing	5
3	Scanning Vulnerabilities Using Tools	5
4	Client-Side Attacks - Social Engineering	10
5	Network Penetration Testing, Detection, and Security	10
6	Man-in-the-Middle Attacks	10
7	Gaining Access to Computer Devices	5
8	Website Penetration Testing, Website Information Gathering	5
9	SQL Injection Vulnerabilities	10
10	Cross-Site Scripting Vulnerabilities	10
11		
Total		٧٥

D. Teaching and Assessment

1. Alignment of Course Learning Outcomes with Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
1.0	**Knowledge**		
1.1	Understand the basics of ethical hacking	Classroom Teaching	Mid Term Exam, Quiz, Final Exam
1.2			
2.0	**Skills**		
2.1	Apply the penetration testing techniques to uncover vulnerabilities in operating systems, applications and networks.	Classroom Teaching/ Lab based Teaching	Mid Term Exam, Quiz, Final Exam, Lab Test, Homework
2.2			
3.0	**Competence**		
3.1	Implement effective countermeasures to defend attacks on operating system and networks based on team engaged work.	Classroom Teaching/ Lab based Teaching	Group Assignment Mini Project Class Test, Mid Exam, Final Exam

2. Assessment Tasks for Students

#	Assessment task*	Week Due	Percentage of Total Assessment Score
1	Quizzes	Week 4, 12	10%
2	Assignments	Week 7, 13	10%
3	Mid Term Exam	Week 8	20%
4	Lab Exercises	Week 7, 13	15%
5	Class Participation	Every Week	5%
6	Final Exam	Week 16	40%
7	**Total**		100%

***Assessment task** (i.e., written test, oral test, oral presentation, group project, essay, etc.)

E. Student Academic Counseling and Support

Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice:
Each student is allotted to an academic advisor for guidance and counselling

F. Learning Resources and Facilities

1. Learning Resources

Required Textbooks	Zaid Sabih,"Learn Ethical Hacking from Scratch", Packt Publishing Ltd, 2018, ISBN 978-1-78862-205-9
Essential Reference Materials	1. Daniel Regalado, Shon Harris, Allen Harper, Chris Eagle, Jonathan Ness, Branko Spasojevic, Ryan Linn, Stephen Sims, "Gray Hat

	Hacking_ The Ethical Hacker's Handbook", McGraw-Hill Osborne Media, 2015 2. Patrick Engebretson,"The Basics of Hacking and Penetration Testing_ Ethical Hacking and Penetration Testing Made Easy", Syngress, 2011
Electronic Materials	
Other Learning Materials	

2. Educational and research Facilities and Equipment Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	Classroom, DF Lab
Technology Resources (AV, data show, Smart Board, software, etc.)	PC or Laptop with Windows/Linux, Smart Board, Projector
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	Internet Connection, DF Lab

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Effectiveness of teaching and assessment	Faculty	Measuring CLO Achievement (Direct)
Extent of achievement of course learning outcomes	Students	CLO Survey (Indirect)
Quality of learning resources	Peers	Final Exam Answer Scripts Verification (Direct)

Evaluation Areas/Issues (e.g., Effectiveness of teaching and assessment, Extent of achievement of course learning outcomes, Quality of learning resources, etc.)
Evaluators (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)
Assessment Methods (Direct, Indirect)

H. Specification Approval Data

Council / Committee	
Reference No.	
Date	

Course specifications

(Postgraduate Degree)

Course Title:	Digital Forensics
Course Code:	DCS 524
Program:	Diploma in Cybersecurity
Department:	Information Technology
College:	College of Computer and Information Sciences
Institution:	Majmaah University

Table of Contents

A. Course Identification

1. Credit hours: 4
2. Course type ☒ Required ☐ Elective
3. Level/year at which this course is offered: Level 2
4. Pre-requisites for this course (if any)**:** N/A
5. Co-requisites for this course (if any)**:** N/A

6. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	**Traditional classroom**	5	100
2	**Blended**	0	0
3	**E-learning**	0	0
4	**Correspondence**	0	0
5	**Other**	0	0

7. Actual Learning Hours (based on academic semester)

No	Activity	Learning Hours
Contact Hours		
1	**Lecture**	45
2	**Laboratory/Studio**	30
3	**Seminars**	0
4	**Others** (specify)	0
	Total	75
Other Learning Hours*		
1	**Study**	45
2	**Assignments**	30
3	**Library**	0
4	**Projects/Research Essays/Theses**	0
5	**Others** (specify)	0
	Total	75

* The length of time that a learner takes to complete learning activities that lead to achievement of course learning outcomes, such as study time, homework assignments, projects, preparing presentations, library times

B. Course Objectives and Learning Outcomes

1. Course Description

This course gives the students a solid foundation to the method of computer forensics and investigations.

It provides an in-depth knowledge of the criminal justice system, computer hardware and software systems, investigative and evidence gathering protocols.

The topics covered will enable the students to possess the knowledge, skills and experience to conduct complex, data-intensive forensic examinations involving various operating systems, platforms and file types.

2. Course Main Objective

- Understand the need and role of digital forensics and computer components like digital media & hard disk basics
- Identify some of the current techniques and tools for forensic examinations & Apply some forensic tools in different situations;
- Describe and identify basic principles of good professional practice for a forensic computing practitioner
- Understanding of professional, ethical, legal, security and social issues and responsibilities in the field of digital forensics.
- Implement forensic analysis, reconstruction, and investigations of digital data in a Windows environment.

3. Course Learning Outcomes

	Course Learning Outcomes (CLOs)	Aligned PLOs*
1	**Knowledge**	
1.1	Understanding of professional, ethical, legal, security and social issues and responsibilities in the field of digital forensics.	K1
2	**Skills**	
2.1	Apply digital forensics tools to investigative and collect evidences.	S1
3	**Competence**	
3.1	Identify the best digital forensic tools and techniques to conduct complex, and data-intensive forensic examinations.	C3

* Program Learning Outcomes

C. Course Content

No	List of Topics	Contact Hours
1	Introduction to digital forensic process and Digital forensic too	6
2	Digital forensics and computer components like digital media & hard disk basics	6
3	File systems (FAT, NTFS, HPFS, HSF etc) and file analysis	10
4	Current techniques and tools for forensic examinations	10
5	Electronic crime scene, Collecting & analyzing electronic evidence	6
6	Digital evidence and Digital investigations	6
7	Investigative reconstruction with digital evidences	10
8	Computer evidence recovery	5
9	Forensic analysis of digital data in a windows environment	6
10	Browser forensics, Audio evidence, Image analysis and Video analysis	10
Total		٧٥

D. Teaching and Assessment

1. Alignment of Course Learning Outcomes with Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
1.0	**Knowledge**		
1.1	Analyze the need and role of digital forensics and computer components like digital media & hard disk basics	Classroom Teaching	Class Test, Mid Exam, Final Exam
1.2	Understanding of professional, ethical, legal, security and social issues and responsibilities in the field of digital forensics.	Classroom Teaching	Class Test, Mid Exam, Final Exam
…			
2.0	**Skills**		
2.1	Apply digital forensics tools to investigative and collect evidences.	Classroom Teaching/ Lab based Teaching	Group Assignment Mini Project Class Test, Mid Exam, Final Exam
3.0	**Competence**		
3.1	Identify the best digital forensic tools and techniques to conduct complex, and data-intensive forensic examinations.	Classroom Teaching/ Lab based Teaching	Group Assignment Mini Project Class Test, Mid Exam, Final Exam

2. Assessment Tasks for Students

#	Assessment task*	Week Due	Percentage of Total Assessment Score
1	Brain storming and review of previous knowledge.	1	-
2	Assignment I/II/III	3,7,12	10%
3	Quiz	6	10%
4	Written Assessment –Mid Term	8	20%
5	Case Study / Exercise Assessment	14	20%
6	Final Exam	15	40%
	Total		100%

***Assessment task** (i.e., written test, oral test, oral presentation, group project, essay, etc.)

E. Student Academic Counseling and Support

Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice:

There will be an academic advisory committee for guidance and counselling

F. Learning Resources and Facilities

1. Learning Resources

Required Textbooks	The Basics of Digital Forensics by John Sammons, 2012, Elsevier Science & Technology
Essential Reference Materials	1. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, Eoghan Casey, Academic Press, 3Ed, 2011 2. Handbook of Computer Crime Investigation: Forensic Tools and Technology, by Eoghan Casey (ed) Butterworth Heinemann 2009.
Electronic Materials	
Other Learning Materials	

2. Educational and research Facilities and Equipment Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	Classroom, DF Lab
Technology Resources (AV, data show, Smart Board, software, etc.)	PC or Laptop with Windows/Linux, Smart Board, Projector
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	Internet Connection, DF Lab

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Effectiveness of teaching and assessment	Faculty	Measuring CLO Achievement (Direct)
Extent of achievement of course learning outcomes	Students	CLO Survey (Indirect)
Quality of learning resources	Peers	Final Exam Answer Scripts Verification (Direct)

Evaluation Areas/Issues (e.g., Effectiveness of teaching and assessment, Extent of achievement of course learning outcomes, Quality of learning resources, etc.)
Evaluators (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)
Assessment Methods (Direct, Indirect)

H. Specification Approval Data

Council / Committee	
Reference No.	
Date	