Course Specification
(Bachelor)

Course Title:	**Cyber threats**
Course Code:	**CYB 0202**
Program:	**Computer Science(Cybersecurity)**
Department:	**Applied Science**
College:	**Applied Collage**
Institution:	**Imam Muhammad Bin Islamic Universirty**
Version:	*Course Specification Version Number*
Last Revision Date:	*Pick Revision Date.*

Table of Contents

A. General information about the course:

1. Course Identification

1. Credit hours: (3(2 Theory, 2 Lab))					
2. Course type					
A.	☐University	☐College	☒ Department	☐Track	☐Others
B.	☒ Required		☐ Elective		
3. Level/year at which this course is offered: (First Semester)					
4. Course General Description:					
This course is designed to introduce students to the concepts of cybercrime including prevention, detection, investigation and incident management processes, policies, procedures and cybercrime governance activities. It therefore focuses on cybercrime management standards, guidelines and procedures. In addition, the course provides students with an understanding of digital investigation techniques for machines, systems and networks.					
5. Pre-requirements for this course (if any)**:**					
CYB 0101 – Information Security Fundamentals					
6. Co-requisites for this course (if any)**:**					
None					
7. Course Main Objective(s):					
The main objective of this course is to provide students with an in-depth understanding of various types of cyber threats, the methods used by attackers, and strategies to mitigate and respond to these threats. This course explores the landscape of cybersecurity threats and equips students with the knowledge and skills necessary to identify, analyze, and combat cyber threats effectively. **By the end of the course, students will be able to:** 1. **Categorize adversary resources, capabilities, techniques** 2. **and motivations.** 3. **List, explain and compare types of cyber attacks.** 4. **Distinguish and identify attack indication events.** 5. **Use cyber threat modeling tools.**					

2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	3 hours\week	100%
2	E-learning		
3	Hybrid • Traditional classroom • E-learning		
4	Distance learning		

3. Contact Hours (based on the academic semester)

No	Activity	Contact Hours
1.	**Lectures**	24
2.	**Laboratory/Studio**	
3.	**Field**	
4.	**Tutorial**	24
5.	**Others (specify)**	
Total		48

B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Code of PLOs aligned with the program	Teaching Strategies	Assessment Methods
1.0	**Knowledge and understanding**			
1.1	Categorize adversary resources, capabilities, techniques and motivations.	**K1**	Lectures, Class Discussions, Case studies and analysis.	Quizzes, Exams, Project, Presentation
1.2	Discuss issues related to ethics and practices of using technology and cybersecurity	**K2**	Lectures, Class Discussions, Case studies and analysis.	Quizzes, Exams, Project, Presentation
1.3	List, explain and compare types of cyber attacks.	**K3**	Lectures, Class Discussions, Case studies and analysis.	Quizzes, Exams, Project, Presentation

Code	Course Learning Outcomes	Code of PLOs aligned with the program	Teaching Strategies	Assessment Methods
	Use cyber threat modeling tools.	**K1**	Lectures, Class Discussions, Case studies and analysis.	Quizzes, Exams, Project, Presentation
2.0	**Skills**			
2.1	Apply critical thinking and problem-solving skills to identify and address cybersecurity challenges.	**S1**	Lectures, Class Discussions, Case studies and analysis.	Quizzes, Exams, Project, Presentation
2.2	Identify different types of attackers and describe their motivations	**S2**	Lectures, Class Discussions, Case studies and analysis.	Quizzes, Exams, Project, Presentation
3.0	**Values, autonomy, and responsibility**			
3.1	Collaboration, teamwork, and professional ethics.	**V1**	Class lectures Class Discussion Questions/Answers sessions in class Home work assignments	Project Writing reports. Study cases.
3.2	Take the responsibility for continuous learning, and self-development.	**V2**	Class lectures Class Discussion Questions/Answers sessions in class Home work assignments	Project Writing reports. Study cases.
3.3	Effective and efficient time management when applying acquired knowledge and skills.	**V3**	Class lectures Class Discussion Questions/Answers sessions in class Home work assignments	Project Writing reports. Study cases.

C. Course Content

No	List of Topics	Contact Hours
1.	Introduction to Cybercrime , Models and Types of Cyber Threats	**2**

2.	Cyber Adversary Model: Resources, Capabilities, Intent, Motivation, Risk Aversion and Access	2
3.	Attack Techniques: Backdoors, Trojans, Viruses, Ransomware, Wireless Attacks, Social Engineering and Covert Channels	4
4.	Password Guessing and Cracking	2
5.	Data Interception, Spoofing and Session Hijacking	2
6.	Data Disclosure, Alteration and Sabotage Threats, Repudiation Threats	4
7.	Denial of Service Attacks, Distributed Denial of Service Attacks and Bots	4
8.	MAC Spoofing, Web Application Attacks, Cloud Computing Attacks and Zero-Day Exploits	2
9.	Advanced Persistent Threats (APT)	2
10.	Attack Indication Events and Attack Timing, Attack Surfaces, Attack Vectors and Attack Trees	4
11.	Insider Threats	4
12.	Threat Information Sources, Strategies and Tools for Developing Cyber Threat Models, Cryptographic Threats	4
13.	Issues Related to the Ethics and Practices of Using Social Media Platforms	4
14.	National and International Legislation to Combat Cybercrimes	4
15.	Legal Issues of Cyber Threats	4
Total		48

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Quizes	3, 8	10%
3.	Midterm	7	20%
4.	Lab Assignments group or individual /Class Assignments group or individual	4,7,9	15%
4.	Lab Evaluations	All Semester	15%
5.	Project	10	10%
6.	Final	13, 14	30%

*Assessment Activities (i.e., Written test, oral test, oral presentation, group project, essay, etc.)

.

E. Learning Resources and Facilities

1. References and Learning Resources

Essential References	BookTitle: Cybersecurity: Attack and Defense Strategies Authors: Yuri Diogenes and Erdal Ozkaya Publisher: Syngress Publication Year: 2019 ISBN: 978-0128114572
Supportive References	https://www.citc.gov.sa/ar/mediacenter/publicationsandbrochures/Documents/PR_PRN_002A.pdf
Electronic Materials	Online resources will be provided during class lectures.
Other Learning Materials	N/A

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	Lecture room with Smart board Lab with 25 Pcs
Technology equipment (projector, smart board, software)	PC and WiFi Internet access within the classroom
Other equipment (depending on the nature of the specialty)	N\A

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Student	Indirect using course evaluation survey
Effectiveness of Students assessment	Student	Indirect using course evaluation survey
Quality of learning resources	Student and Faculty	Indirect using course evaluation and faculty survey
The extent to which CLOs have been achieved		
Other		

Assessors (Students, Faculty, Program Leaders, Peer Reviewers, Others (specify)

Assessment Methods (Direct, Indirect)

G. Specification Approval

COUNCIL /COMMITTEE	
REFERENCE NO.	
DATE	