هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

2023
TP-153

Course Specification
(Bachelor)

Course Title::	**Cyber Security and Cyber Crime**
Course Code:	**ITEC 333**
Program:	**Bachelor in Information Technology (BIT)**
Department: :	**Information Technology and Security**
College:	**Computer Science and Information Technology**
Institution:	**Jazan University**
Version:	**1**
Last Revision Date:	**10/5/2024**

Table of Contents

A. General information about the course:

1. Course Identification

1. Credit hours: (3)					
2. Course type					
A.	☐University	☐College	☒ Department	☐Track	☐Others
B.	☐Required		☒ Elective		
3. Level/year at which this course is offered: (Level 6. Year 3)					
4. Course general Description:					

This course explores cyber-security measures and the different forms of cybercrime and emergent forms of cyber-warfare. Students will learn challenges to cyber-security and examine the nature, prevalence, scope and the means by which criminals perform these crimes. They will be aware of how the concept of cyber power rises naturally from a holistic consideration of cybersecurity and, specifically, how it can be expressed through cyber criminality, cyberterrorism, cyber conflicts and cyberwarfare. The course also provides the impact of cybercrime on victims, business, and the state, and the responses of information security providers and police agencies. Ethics and laws related to cyber crime are also introduced. The course concludes with a critical assessment of the threats to rights posed by the emergent new digital age of surveillance.

5. Pre-requirements for this course (if any)**:**

ITEC-331, Fundamentals of IT Security

6. Co-requirements for this course (if any)**:**

NIL

7. Course Main Objective(s):

- **Understand the context of emerging crime threats and technological and other trends in cyberspace.**
- **Understand the threats that society should be prepared to face and the ways in which crimes and conflicts are carried out in cyberspace.**
- **Respond to cyberattacks and ensure cybersecurity strategies.**
- **Distinguish and classify the forms of cybercriminal activity and the methods used to undertake such crimes.**
- **Investigate assumptions about the behavior and role of offenders and victims in cyberspace and use basic web-tools to explore behavior on-line.**
- **Develop the awareness and skills that will allow society to fight against cyber-based criminality and abuse.**
- **Analyze and assess the impact of cybercrime on government, assets, individuals, and society.**
- **Evaluate the effectiveness of cyber-security ethics, cyber-laws and other counter measures against cybercrime and cyber warfare.**

2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	30T + 26 L	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**	30
2.	**Case Study/Laboratory/Studio**	26
3.	**Field**	
4.	**Tutorial**	
5.	**Others (specify) Exams**	4
Total		60

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

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods	ABET Student Outcomes (SOs)
1.0	**Knowledge and understanding**				
1.1	Define the fundamentals of cyber security, cyber crime, defense, and ethics	CLO-1 (K1)	Visual & Verbal [Lectures/ Presentations]	Midterm Exam, Final Exam Assignment,	**SO-4**
1.2	Recognize the recent trends in Cyber security and cybercrime.	CLO-2 (K2)	Visual & Verbal [Lectures/ Presentations]	Midterm Exam, Assignment, Case Studies, Final Exam	**SO-4**
2.0	**Skills**				
2.1	Analyze Cyber security Incidents response plans and application of	CLO-3 (S4)	Visual & Verbal [Lectures/ Presentations]	Assignment, Case Studies, Final Exam	**SO-6**

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods	ABET Student Outcomes (SOs)
	appropriate security measures and tools				
2.2	Use security principles to mitigate cybercrimes against persons, assets, and government.	CLO-4(S4)	Visual & Verbal [Lectures/ Presentations]	Assignment, Case Study, Final Exam	**SO-6**
2.3	Evaluate global approach to cyber security, cyber crime laws and ethics.	CLO-5(S3)	Group meetings/Work breakdown structuring among the team members	Assignment, Case Study, Final Exam	**SO-2**
3.0	Values, autonomy, and responsibility				
3.1	Demonstrate the ability to function effectively as a member or leader of a team to recognize, discuss, present and evaluate cyber security-based issues and their solutions.	CLO-6 (V2)	Active class participation in group Activities	Case Study Group discussion/ presentation	**SO-5**

C. Course Content

No	List of Topics	Contact Hours
1.	Chapter 01- Understanding fundamentals of Cyber Security and Cyber crimes	5T+4P
2	Chapter 02 –Recent trends in cybersecurity and cybercrime	5T+4P
3	Chapter 03 - Managing the security problems and Security tools	5T+4P
4	Chapter 04 - Cybercrimes Against Persons , Assets and States	5T+4P
5	Chapter 05: Ethics and Laws relating to Cyber security and Cybercrime	5T+4P
6	**Revision (if required)+ Exams (midterm, case study, Final)**	5T+2 P 4 Exams
Total		**30 Th+ 26P + 4** =60

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1	**Assignment** 1	**4**	**10%**
2	**Mid-exam**	**7**	**15** %
3	**Assignment** 2	**10**	**15** %
4.	**Case study Exam** (Internal assessment + Final Report and Presentation)	**12**	**10+10=20%**
5.	**Final Exam**	**14-15**	40%

*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	Cyber Power CRIME, CONFLICT AND SECURITY IN CYBERSPACE, SOLANGE GHERNAOUTI- CRC PRESS
Supportive References	• Cybercrime and Society (4th ed.), Majid Yar, Kevin F. Steinmetz (2024) • Cybercrime and Cybersecurity, ByPaul A. Watters, Edition1st Edition, 2023 • Cybercrime: The Transformation of Crime in the Information Age, 2nd Edition, David S. Wall , ISBN: 978-1-509-56313-5, April 2024
Electronic Materials	https://me-en.kaspersky.com/resource-center/threats/what-is-cybercrime https://www.itworldcanada.com/article/cyber-security-today-year-in-review-for-2022/519705
Other Learning Materials	--

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	Classrooms
Technology equipment (projector, smart board, software)	Projector, Smart board, Blackboard (LMS)
Other equipment (depending on the nature of the specialty)	--

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Students, HoD	In-Direct/Direct
Effectiveness of students assessment	Faculty	Direct
Quality of learning resources	Program Leaders	Direct
The extent to which CLOs have been achieved	Program Leaders	Direct
Other	--	--

Assessor (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)
Assessment Methods (Direct, Indirect)

G. Specification Approval

COUNCIL /COMMITTEE	
REFERENCE NO.	
DATE	