هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

اعتماد
NCAAA

2023

TPG-153

Course Specification

(Postgraduate)

Course Title: Fundamental of cybersecurity	
Course Code: CYBS60101	
Program: M.Sc. in Cybersecurity	
Department: Department of Computer Science	
College: Faculty of Computing and Information	
Institution: Al Baha University	
Version: 1	
Last Revision Date: 12-12-2023	

Table of Contents

A. General information about the course:

1. Course Identification:

1. Credit hours: (3)					
3 Hours					
2. Course type					
A.	☐University	☐College	☐Department	☐Track	
B.	☒ Required		☐Elective		
3. Level/year at which this course is offered: (1/1^{t})					
4. Course general Description:					
This course provides general knowledge of basic concepts in cybersecurity. It discusses Cybersecurity principles, threats, and vulnerabilities. The course explores data protection and recent topics in the field of cybersecurity. Besides, important concepts like Encryption, risk management, Incident response, and social engineering will be briefly covered to equip students with the necessary knowledge to explore the field of cybersecurity.					
5. Pre-requirements for this course (if any):					
None					
6. Co-requirements for this course (if any):					
None					

7. Course Main Objective(s):

The students completed this course will be able to:

- Explain basic terms and concepts in the field of cybersecurity.
- Explain the characteristics and value of personal data, and data within an organization.
- Review cyber risks, threats and vulnerabilities.
- Explain the methodologies and techniques used to protect data, systems, and networks.
- Discuss appropriate procedures for managing cyber risks and responding to cyber incidents.
- Recognize the behavior-based approach to cybersecurity.

2. Teaching Mode: (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	26	80%

No	Mode of Instruction	Contact Hours	Percentage
2	E-learning	7	20%
3	Hybrid □ Traditional classroom □ E-learning		
4	Distance learning		

3. Contact Hours: (based on the academic semester)

No	Activity	Contact Hours
1.	**Lectures**	33
2.	**Laboratory/Studio**	-
3.	**Field**	-
4.	**Tutorial**	-
5.	**Others (specify)……**	-
	Total	33

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

Code	Course Learning Outcomes	Code of PLOs aligned with program	Teaching Strategies	Assessment Methods
1.0	**Knowledge and understanding**			
1.1	Describe fundamental terms and ideas in cybersecurity.	**K1**	• Lectures • Assignments	• Quizzes • Midterm Exam • Final Exam
1.2	Explain the characteristics and value of personal data, and data within an organization.	**K2**	• Lectures • Assignments	• Quizzes • Midterm Exam • Final Exam
1.3	Evaluate cybersecurity risks, threats, and vulnerabilities.	**K3**	• Lectures • Assignments	• Quizzes • Midterm Exam • Final Exam
2.0	**Skills**			
2.1	Demonstrate the methods and strategies employed for safeguarding data, systems, and networks.	**S1**	• Lectures • Assignments	• Quizzes • Midterm Exam • Final Exam

Code	Course Learning Outcomes	Code of PLOs aligned with program	Teaching Strategies	Assessment Methods
2.2	Discuss suitable processes for handling cyber risks and reacting to cyber events.	S2	- Lectures - Assignments	- Quizzes - Midterm Exam - Final Exam
2.3	Recognize the behavior-based approach to cybersecurity.	S3	- Lectures - Assignments	- Quizzes - Midterm Exam - Final Exam
3.0	Values, autonomy, and responsibility			
3.1	Make the assigned tasks on time within a team and communicate effectively in written project reports and oral presentations.	V1	- Assignments (Group) - Project (Group)	- Reports - Presentations - Class Discussions

C. Course Content:

No	List of Topics	Contact Hours
1.	The Importance of Cybersecurity and its Design Principals	3
2.	Cyber Risks, Threats and Vulnerabilities	3
3.	Maintaining Confidentiality, Integrity and Availability and Beyond	3
4.	Control Access, Authentication, Authorization and Non-Repudiation	3
5.	Encryption and Its Uses	3
6.	Governance and Cyber Risk Management	3
7.	Protecting the Organization (Data, Systems and Networks)	3
8.	Security Know-How and Cyber Threats Monitoring	3
9.	Incident Response	3
10.	Technologies and Solutions Used in Cybersecurity and Recent Occurrences of Security Breaches	3
11.	Social Engineering and the Effect of the Human Factor in Cybersecurity	3
Total		33

D. Students Assessment Activities:

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Assignments	Every two weeks	5%
2.	Report, presentation, and Class Discussions	Week 10	5%
3.	Midterm Exam	Within the 6th Week	20%
4.	Quiz	Week 8	10%
5.	Project	Week 11	10%
6.	Final Exam	Week 13	50%

*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	□ Computer Security: Principles and Practice, 4th edition by William Stallings, Lawrie Brown, 2018. □ Michael E. Whitman and Herbert J. Mattord – Principle of Information Security – Second Edition –Thomson Course Technology
Supportive References	□ Communications of ACM (Association for Computer Machinery) - http://cacm.acm.org/ □ Journal of the ACM - http://jacm.acm.org/
Electronic Materials	□ Access to the Saudi Digital Library (SDL). □ Using the learning management system of the university – Rafid System (https://lms.bu.edu.sa/). □ IEEE/ACM Transactions on Networking https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=90
Other Learning Materials	

2. Educational and Research Facilities and Equipment Required:

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	• A classroom or lecture hall with whiteboard for 25 students. • A laboratory with 25 computers.
Technology equipment (Projector, smart board, software)	All students shall have • A laptop or access to a desktop computer with access to a programming development tool • High speed Internet connection • Power outlets for student's laptop plug-in • Relevant programming software for use of students.

Items	Resources
Other equipment (Depending on the nature of the specialty)	• The laboratory should have computers with programming development tools.

F. Assessment of Course Quality:

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Students - Program Leaders	Indirect
Effectiveness of students' assessment	Program Leaders	Indirect
Quality of learning resources	**Students**	**Indirect**
The extent to which CLOs have been achieved	Peer reviewers	Direct
Reviewing course effectiveness and planning for improvement.	Program Leaders - Faculty	Direct

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

G. Specification Approval Data:

COUNCIL /COMMITTEE	
REFERENCE NO.	
DATE	