2023
TP-153

Course Specification
(Bachelor)

Course Title:	Introduction to Cybersecurity
Course Code:	SE1752
Program:	Bachelor of Software Engineering
Department:	Software Engineering
College:	Faculty of Computers and Informatics
Institution:	Al-Baha University
Version:	1.0
Last Revision Date:	23/4/2024

Table of Contents

A. General information about the course:

1. Course Identification

1. Credit hours: (.....)					
2. Course type					
A.	☐University	☐College	☒ Department	☐Track	☐Others
B.	☒ Required		☐Elective		
3. Level/year at which this course is offered: (9)					
4. Course general Description:					
Overview of the evolving cyberspace ecosystem, the interoperability of physical and social networks, and methods and techniques in securing that ecosystem. Explore briefings of the ethical, legal, and technical aspects of cybercrime and methods of prevention, detection, response and recovery. The value of strong moral character, integrity, and trust as prized attributes of cybersecurity practitioners will be highlighted. Essential cybersecurity topics overview including operating system models and mechanisms for mandatory and discretionary controls, data models, basic cryptography and its applications, security in computer networks and distributed systems, inspection and protection of information assets, detection of and reaction to threats to information assets, and examination of pre- and postincident procedures, technical and managerial responses, information security planning and staffing functions, data mining and data science, and policy and assurance issues. Being prepared as life-long learner tailored to their academic/career goals.					
5. Pre-requirements for this course (if any)**:**					
Software Security (SE1507)					
6. Pre-requirements for this course (if any)**:**					
none					
7. Course Main Objective(s):					

Teaching Cybersecurity fundamentals to be motivated to begin career as Cybersecurity professional.

2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	3	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**	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 CLOs aligned with program	Teaching Strategies	Assessment Methods
1.0	**Knowledge and understanding**			
1.1	**Recognize knowledge of cybersecurity concepts and terminology as well as get idea**	**K1**	**Course lectures, tutorials, HomeWorks, term project**	**Quiz, Exam**

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
	about digital forensics and available tools to serve its applications.			
1.2	Describe needs to secure information while preserving legal and regulatory requirements in Saudi Arabia and Internationally.	K2	Course lectures, tutorials, HomeWorks, term project	Quiz, Exam
1.3	Describe generally the vulnerabilities and sources of attack risking digital systems.	K3	Course lectures, tutorials, HomeWorks, term project	Quiz, Exam
2.0	**Skills**			
2.1	Employ basic security principles and practices integrated to knowledge of computing and information technologies to serve against cybersecurity problems	S1	Tutorial Term project	HomeWorks
2.2	Analyze in very simplified manner the cyber computing-based solution to protect information under risks situations.	S2	Tutorial Term project	HomeWorks
2.3	Analyze generally the legal and regulatory	S3	Tutorial Term project	HomeWorks

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
	requirements related to cybersecurity computer systems and digital evidence.			
	Function orally to accomplish common goals.	S4	Open Related Topic General Coverage	Oral presentation
3.0	Values, autonomy, and responsibility			
3.1	Engage in lifelong learning for continued professional excellence.	V1	Open Related Topic General Coverage	Oral presentation

C. Course Content

No	List of Topics	Contact Hours
1.	Introduction to Cybersecurity specialization	5
2.	Cybersecurity Fundamentals and CIA	5
3.	Cyberthreat Prevention, Detection, Recovery	6
4.	Enterprise Architecture and Components	6
5.	Information System Governance and Risk Assessment	6
6.	Incident Management	5
Total		33

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Quizzes	3, 8	10%
2.	Midterm	6	25%
3.	HomeWorks	10	10%
4.	Oral presentation	10	20%
5.	Final Exam	12	35%

*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	**Introduction to Cyber Security: Fundamentals By Ugo Ekpo, 2018 - ISBN: 978-1728711621**
Supportive References	**N/A**
Electronic Materials	**Rafid**
Other Learning Materials	**N/A**

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	**Classroom**
Technology equipment (projector, smart board, software)	**Data show, Software**
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	- Survey
Effectiveness of Students assessment	- Lecturer	- Annual report
Quality of learning resources	- Program Coordinator	- Survey - Evaluation of test - Models Standard sample
The extent to which CLOs have been achieved		
Other		

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

Assessment Methods (Direct, Indirect)

G. Specification Approval

COUNCIL /COMMITTEE	**Curriculum Committee**
REFERENCE NO.	

DATE	**28 April 2024**