Course Specification
(Bachelor)

Course Title:	Fundamentals of Cybersecurity
Course Code:	331CCN-3
Program:	Bachelor of Science in Computer Networks
Department:	Networks and Communications Engineering
College:	Computer Science and Information Systems
Institution:	Najran University
Version:	1.0
Last Revision Date:	15 February 2025

Table of Contents

A. General information about the course:

1. Course Identification

1. Credit hours: (3 (2, 2, 1) [Theory, Lab, Tutorial])					
2. Course type					
A.	☐University	☒ College	☐Department	☐Track	☐Others
B.	☒ Required		☐Elective		
3. Level/year at which this course is offered: (Level 5/ Year 3)					
4. Course General Description:					
Study of common Abstract Data Types (ADTs), basic data structures and design and analysis of algorithms. Common ADTs: stack, queue, list, tree, priority queue, map and dictionary. Basic Data structures include arrays, linked lists, heaps, hash tables, search trees. Basic design and analysis of algorithms covers asymptotic notation, recursive algorithms, searching and sorting, tree traversal, graph algorithms.					
5. Pre-requirements for this course (if any):					
٢٠١CCN-3					
6. Co-requisites for this course (if any):					
N/A					
7. Course Main Objective(s):					
The main objective of this course is to equip students with a solid foundational understanding of cybersecurity principles and techniques, focusing particularly on cryptography, threat assessment, risk management, and incident response. Students will develop the skills necessary to identify, analyze, and mitigate potential cyber threats, ensuring the protection of digital assets for individuals and organizations in an evolving technological landscape.					

2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	75	١٠٠%
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**	[2 contact hours ´ 15 weeks]	30
2.	**Laboratory/Studio**	[2 contact hours ´ 15 weeks]	30
3.	**Field**		
4.	**Tutorial**	[1 contact hour ´ 15 weeks]	15
5.	**Others (specify)**		
Total			**Total**

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	Demonstrate a comprehensive understanding of core cybersecurity principles, including cryptography, risk assessment, and threat identification, enabling the evaluation and implementation of security measures in diverse digital environments.	K2	Lecture	Tests, Quizzes, and Assignments Tests, Quizzes, andAssignments
1.2	Define the concepts of authentication and access control	K1, K2		
1.3	Understanding of Cryptographic Principles: Students will grasp the fundamental	K1, K2		Tests, Quizzes, and Assignments

Code	Course Learning Outcomes	Code of PLOs aligned with the program	Teaching Strategies	Assessment Methods
	principles of cryptography, including encryption techniques, cryptographic algorithms, and their applications in securing data. They will comprehend how cryptographic methods contribute to maintaining confidentiality, integrity, and authentication in digital communications and storage.			
...				
2.0	**Skills**			
2.1	Implement cryptographic techniques and security measures proficiently to prevent unauthorized access and enhance data protection.	S4	Lecture, Lab	Tests, Quizzes, Assignments, and Lab
2.2	Conduct thorough risk assessments and vulnerability analyses for robust threat identification and fortification of digital systems.	S4		
2.3	Design and execute swift incident response plans, showcasing effective problem-solving and cybersecurity	S1, S6		

Code	Course Learning Outcomes	Code of PLOs aligned with the program	Teaching Strategies	Assessment Methods
	incident management skills.			
3.0	**Values, autonomy, and responsibility**			
3.1				
3.2				
...				

C. Course Content

No	List of Topics	Contact Hours
1	Introduction to Cybersecurity	5
2	Understanding Cyber Threats and Attack Vectors	5
3	Cryptography Basics and Encryption Techniques	5
4	Risk Management in Cybersecurity	5
5	Network Security Principles	5
6	Access Control and Authentication Methods	5
7	Security Architecture and Design Principles	5
8	Malware Detection and Prevention	5
9	Security for Web and Mobile Applications	5
10	Incident Response and Handling	5
11	Social Engineering and Insider Threats	5
12	Compliance and Legal Aspects in Cybersecurity	5
13.	Emerging Trends and Technologies in Cybersecurity	5
14	Ethical Considerations in Cybersecurity Practices	5
15	Practical Applications and Case Studies in Cybersecurity.	5
Total		75

D. Students Assessment Activities

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

E. Learning Resources and Facilities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Quizzes	2, 4, 8,10	8%
2.	Assignments or mini project (presentation)	3, 5, 8, 9	12%
3.	Midterm Examination	6th week	20%
4.	Lab Activities	1-14th week	10%
٥.	Lab Final Examination	15th week	10%
6.	Final Examination	16th,17th week	40%

1. References and Learning Resources

Essential References	1. "**Principles of Computer Security: CompTIA Security+ and Beyond**" by Wm. Arthur Conklin, Greg White, Chuck Cothren, Roger L. Davis, Dwayne Williams. (Edition: 5th Edition, Publication Year: 2018) "Cryptography and Network Security: Principles and Practice" by William Stallings. (Edition: 7th Edition, Publication Year: 2016)
Supportive References	• "**Cybersecurity Essentials**" by Charles J. Brooks. (Edition: 2nd Edition, Publication Year: 2017) "**Introduction to Cybersecurity**" by Robert M. Jones. (Edition: 1st Edition, Publication Year: 2014)
Electronic Materials	Available in Blackboard
Other Learning Materials	

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	Lecture Room and Laboratory
Technology equipment (projector, smart board, software)	data show, PCs.
Other equipment (depending on the nature of the specialty)	Network Security Lab

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Students	• Indirect (questionnaire) • University online questionnaire for evaluation the course by students. • Observing the student's opinions recorded on the college student site. Appeal & suggestions box
Effectiveness of Students assessment	Peer reviewer	Direct (review of the quality of the exam done by the course coordinator)
Quality of learning resources	Faculty & students	Lecturers prepare and create the learning resources before the class begins and make them more related to the course. Questionnaire
The extent to which CLOs have been achieved	Faculty	Student assessments reviewing
Other		

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

Assessment Methods (Direct, Indirect)

G. Specification Approval

COUNCIL /COMMITTEE	NETWORK AND COMMUNICATIONS ENGINEERING DEPARTMENT COUNCIL
REFERENCE NO.	**14450824-0482-00014**
DATE	**5/3/2024**