Course Specification
(Bachelor)

Course Title:	Cyber Security
Course Code:	IS 1388
Program:	Bachelor of Information Systems
Department:	Information systems
College:	College of Computer and Information Sciences
Institution:	Imam Mohammad Ibn Saud Islamic University
Version:	1
Last Revision Date:	

Approved: 24/08/2025

Table of Contents

A. General information about the course:

1. Course Identification

1. Credit hours: 3 credit hours (lectures:3)

2. Course type

A.	☐University	☐College	☒ Department	☐Track	☐Others
B.	☐ Required		☒ Elective		

3. Level/year at which this course is offered: 3rd Year

4. Course general Description

This course aims to provide students with an academic overview of cyber security covering its main domains. The course provides the foundation for understanding the key issues associated with protecting information and assets on operating system, determining the authentication and authorization techniques for safe access to information. In addition, the course will provide student with practical hints and experience of emerging topics of cyber security. Moreover, strategic defenses will be observed on broad level.

By the completion of this course, students should appreciate the significance of cyber security in the IT realm, and be able to demonstrate in-depth knowledge of cyber security technical key principles and techniques. Upon successful completion of this course, students will have a broad ethical knowledge of the major technical security challenges.

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

IS1321 Databases Management Systems
IS1330 Fundamentals of Data Networks

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

No Co-requisites

7. Course Main Objective(s):

The target of the course is to introduce topics related to cyber security. The students will learn about cyber security terminologies, basic cryptography techniques, access control authorization and authentication, some direct emerging topics of cyber security, malicious software, ethical hacking overview, cyber security ethics and laws and cyber security systems development project.

2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	3 hours/week	100%

No	Mode of Instruction	Contact Hours	Percentage
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**	45
2.	**Laboratory/Studio**	
3.	**Field**	
4.	**Tutorial**	
5.	**Others (specify)**	
Total		45

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	*Define the fundamental concepts, methods, and practice of cybersecurity; also list the main characteristics of social engineering and malicious software.*	K1(P)	Class lectures	*Written Exams (Midterm and Final)*
1.2	*Demonstrate the key concepts of cybersecurity*	K2(P)	Class lectures	*Written Exams (Midterm and Quiz)*

	operating systems, networks, and strategic cyber defense mechanisms.			
1.3	*Demonstrate a comprehensive understanding of security risk management, cyber policies, and incident response principles.*	K1(P), K3(I)	Class lectures	*Written Exams (Midterm and Final)*
1.4	*Identify emerging trends and technologies in the field of cybersecurity*	K3(I)	Class lectures	*Written Exams (Final)*
1.5	*Recognize legal, ethical, and regulatory principles governing cybersecurity and cybercrime*	K2(P)	Class lectures	*Written Exams (Quiz and Final)*
2.0	**Skills**			
2.1	*Conduct security assessments and audits to evaluate adherence to cybersecurity standards and regulations.*	S1(I)	Class lectures	*Assignment*
2.2	*Develop incident response plans and procedures for cyber attack scenarios.*	S2(I), S4(I)	Class lectures	*Assignment*
3.0	**Values, autonomy, and responsibility**			
3.1	*Function effectively on teams to accomplish common cybersecurity objectives.*	V1(P)	Class Discussion and lectures	**Project Report**

3.2	*Present cybersecurity topics and solutions in a clear and compelling manner.*	V3(P)	lectures	**Project Presentation**

C. Course Content

No	List of Topics	Contact Hours
1.	Introduction to cybersecurity & Threat Landscape	4
2.	Cyber Attacks & Malware Ecosystem	5
3	Network & Infrastructure Security	5
4	Web & Application Security	4
5	Identity, Access & Trust Management	4
6	Security Risk Management & Cyber Policies	4
7	Incident Response, Digital Forensics & Cyber Resilience	5
8	Social Engineering, Human Factors & Insider Threats	4
9	Cyber Laws, Ethics & Compliance	3
10	Emerging Trends in Cyber Security	4
11	Project Discussion	3
Total		**45**

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	**Quiz**	4,11	10%
2.	**Midterm Exam**	8	20%
3.	**Assignment**	7	10%
4	**Group Project**	15	20%
5	**Final Exam**	16	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	Cybersecurity Essentials, Second Edition; Charles J. Brooks, Christopher Grow, Philip Craig Jr., Donald Short, Published 2018

	by Cisco Press; ISBN-10: 013518591X, ISBN-13: 978-0135185919. Computer Security: Principles and Practice, Fourth Edition; William Stallings, Lawrie Brown, Published 2018 by Pearson Education; ISBN-10: 0134794106, ISBN-13: 978-0134794105.
Supportive References	Security in Computing, Fifth Edition; Charles P. Pfleeger Shari Lawrence Pfleeger Jonathan Margulies, Published January, 2015 by Pearson Education;ISBN-10: 0-13-408504-3, ISBN-13: 978-0-13-408504-3 Cybersecurity and Cyberwar: What Everyone Needs to Know; P. W. Singer, Allan Friedman, Published 2014 by Oxford University Press; ISBN-10: 019991811X, ISBN-13: 978-0199918119.
Electronic Materials	**N/A**
Other Learning Materials	**N/A**

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	**1. At least 30 seats** **2. A projector connected to a PC preferably with Internet connection** **3. Sliding board**
Technology equipment (projector, smart board, software)	**N/A**
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	**Students**	**Indirect using course evaluation survey**
Effectiveness of Students assessment	**Faculty members**	**Direct method using TOS file**
Quality of learning resources	**Students and Faculty**	**Indirect using course evaluation survey and faculty survey**
The extent to which CLOs have been achieved	**Faculty members**	**Direct method using TOS file**
Other		

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

Assessment Methods (Direct, Indirect)

G. Specification Approval

COUNCIL /COMMITTEE	**IS CURRICULUM APPROVAL & DEVELOPMENT COMMITTEE IS QAC / / IS COUNCIL**
REFERENCE NO.	
DATE	