KINGDOM OF SAUDI ARABIA
IMAM MOHAMMAD IBN SAUD ISLAMIC UNIVERSITY
COLLEGE OF COMPUTER SCIENCE AND INFORMATION
COMPUTER SCIENCE DEPARTMENT
BACHELOR OF COMPUTER SCIENCE

المملكة العربية السعودية
جامعة الإمام محمد بن سعود الإسلامية
كلية علوم الحاسب والمعلومات
قسم علوم الحاسب
بكالوريوس علوم الحاسب

SYLLABUS

IS 380: Cybersecurity

PREREQUISITE	*IS321, CS330*	CREDIT HOURS	3

Instructor:
Contact information and office hours
Office No: 2077
Office Hours: Monday & Wednesday 12:00 PM Until 1:30 PM
E-mail: talzahrani@imamu.edu.sa

COURSE DESCRIPTION
This course aims to provide students with an academic overview of cybersecurity 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 cybersecurity. Moreover, strategic defenses will be observed on broad level.   *By the completion of this course, students should appreciate the significance of cybersecurity in the IT realm, and be able to demonstrate in-depth knowledge of cybersecurity technical key principles and techniques. Upon successful completion of this course, students will have a broad ethical knowledge of the major technical security challenges.*

	COURSE LEARNING OUTCOMES (CLOs)	Aligned SOs
1	**Knowledge and Understanding**	
1.1	*Define the fundamental concepts, methods, and practice of cybersecurity.*	1(I)

1.2	*Outline the key concepts of cybersecurity operating systems and strategic defence.*	1(I)
1.3	*Describe the fundamental issues in designing access control models and authentication.*	1(I)
1.4	*List the main characteristics of social engineering and malicious software*	1(I)
1.5	*State cybersecurity regulation, ethics and laws.*	4(P)
2	**Skills :**	
2.1	*Explain the basic cryptography concepts.*	1(I)
2.2	*Plan and organize an information systems cybersecurity development project.*	2(P), 6(P)
3	**Values:**	
3.1	*Function effectively on teams to accomplish a common goal.*	5(P)
3.2	*Present a topic in a compelling manner.*	3(P)

TEACHING Strategies

In face-to-face lectures, during lectures, the instructor includes demos and practical sessions for cybersecurity.
Self-learning.

No	List of Topics	Contact Hours
1	Introduction to cybersecurity	*3*
2	Basic Cryptography	*3*
3	Operating System Security	*3*
4	Strategic Defenses	*3*
5	Access Control-Authentication	*3*
6	Access Control-Authorization	*6*
7	Cybersecurity Emerging topics	*6+3*
8	Social Engineering and malware	*3+3*
9	Cybersecurity Frameworks, Ethics and Laws	*3*
10	Project Discussion	*3*
Total		*36+6(SL)*

TEXT BOOK

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

REFERENCES

● *Understanding Cryptography, 1 edition, ChristofPaar; Jan Pelzl, Springer, 2010, ISBN 978-3642041006.*
● *Computer Security, 3rd edition, Dieter Gollmann, John Wiley&Sons, 2011, ISBN 978-0470741153.*
● *Information Security Principles and Practice, 2nd edition, Mark Stamp, Wiley Publications, 2011, ISBN 978-0470626399.*

No	Assessment Method	Due Week	%Total Assessment
	Course Assessment Methods		
1	Quiz	4	10
2	Assignment	9	10
3	Midterm	7	20
4	Project / Lab Exam	12	20
5	Final Exam	13	40