

ATTACHMENT 5.

Kingdom of Saudi Arabia
**The National Commission for Academic Accreditation &
Assessment**

T6. Course Specifications (CS) of
“IS 384- Information Security”

College of Computer and Information Systems

Al Yamamah University

Riyadh, KSA

March 26, 2016

Course Specifications

Institution	Al-Yamamah University Riyadh KSA	Date: 3/4/2016
College/Department : College of Computer and Information Systems		

A. Course Identification and General Information

1. Course title and code: Information Security and ISY 384			
2. Credit hours. 3			
3. Program(s) in which the course is offered. (If general elective available in many programs indicate this rather than list programs)			
4. Name of faculty member responsible for the course			
5. Level/year at which this course is offered			
6. Pre-requisites for this course (if any) ISY 102			
7. Co-requisites for this course (if any) N/A			
8. Location if not on main campus			
9. Mode of Instruction (mark all that apply)			
a. traditional classroom	<input checked="" type="checkbox"/>	What percentage?	<input type="text" value="100"/>
b. blended (traditional and online)	<input type="checkbox"/>	What percentage?	<input type="text"/>
c. e-learning	<input type="checkbox"/>	What percentage?	<input type="text"/>
d. correspondence	<input type="checkbox"/>	What percentage?	<input type="text"/>
f. other	<input type="checkbox"/>	What percentage?	<input type="text"/>
Comments:			

B Objectives

1. What is the main purpose for this course?

This course is designed to look at management issues and practical implications related to securing information systems. This course focuses on the explanation and develops understanding of technical terms used in field of security. A clear theoretical understanding supports a large practical component where students learn to use and audit information systems and use contemporary security software.

This course is designed to develop sound understanding of Information Security and vulnerability assessment and develop secure operation environment for corporate level applications.

The course is ideal for those who are interested in helping organizations protect critical information assets and secure their systems both by recognizing current threats and vulnerabilities, and by designing and developing the secure systems of the future.

2. Briefly describe any plans for developing and improving the course that are being implemented. (e.g. increased use of IT or web based reference material, changes in content as a result of new research in the field)

Since this course is being offered for the first time in Information Systems Program and content / course learning outcomes will be revised. There will be a special survey for students of IS478 in almost 14 – 15 week , asking them for their recommendations, feedback and if there is something valuable that will be added to the content or course learning outcomes.

C. Course Description (Note: General description in the form used in Bulletin or handbook)

Course Description:

This course will provide a comprehensive introduction and study into a broad selection of contemporary information systems security issues, concepts and policies, including the survey of state-of-the art technology used to address security problems. Topics of study include core security mechanisms of access control and integrity, basic cryptography techniques, assurance, authentication, digital signatures and database security mechanisms. The course discusses security policy and privacy issues for information systems protection and detection, as well as an overview of recent trends in commercial products and applications and security research in basic network security, intrusion detection.

1. Topics to be Covered		
List of Topics	No. of Weeks	Contact hours
Introduction and study into a broad selection of contemporary information systems	1	3
Security issues, concepts and policies, including the survey of state-of-the art technology used to address security problems	2	6
Topics of study include core security mechanisms of access control and integrity	2	6
Basic cryptography techniques	2	6
Assurance, authentication, digital signatures	2	6
Database security mechanisms	2	6
Security policy of organizations Information systems	1	3
Privacy issues for information systems and protection	1	3
Recent trends in commercial products and applications	1	3
Current research in security research for basic network security, intrusion detection	1	3

2. Course components (total contact hours and credits per semester):						
	Lecture	Tutorial	Laboratory or Studio	Practical	Other:	Total
Contact Hours	3					3
Credit						

3. Additional private study/learning hours expected for students per week.	2
--	---

4. Course Learning Outcomes in NQF Domains of Learning and Alignment with Assessment Methods and Teaching Strategy

On the table below are the five NQF Learning Domains, numbered in the left column.

First, insert the suitable and measurable course learning outcomes required in the appropriate learning domains (see suggestions below the table). **Second**, insert supporting teaching strategies that fit and align with the assessment methods and intended learning outcomes. **Third**, insert appropriate assessment methods that accurately measure and evaluate the learning outcome. Each course learning outcomes, assessment method, and teaching strategy ought to reasonably fit and flow together as an integrated learning and teaching process. (Courses are not required to include learning outcomes from each domain.)

Code #	NQF Learning Domains And Course Learning Outcomes	Course Teaching Strategies	Course Assessment Methods
1.0	Knowledge		
1.1	Define key terms and concepts of information security, and demonstrate that organizations have a need for information security.	<ul style="list-style-type: none"> • Lectures • Discussion-Based Teaching 	<ul style="list-style-type: none"> • Homework assignments • In class short MCQs quizzes •
1.2	Identify the threats posed to information security and the more common attacks associated with those threats. Describe protection methods and technologies	<ul style="list-style-type: none"> • Lectures • Active and Collaborative Learning • Problem solving cases • Independent study (project) 	<ul style="list-style-type: none"> • Homework assignments • In class short MCQs quizzes • Presentation by the students • Midterm exam • Final Exam
2.0	Cognitive Skills		
2.1	Solve problems within the context of information security	<ul style="list-style-type: none"> • Lectures • Problem solving cases • Class discussions • Independent study (project) 	<ul style="list-style-type: none"> • Presentation by the students • Examinations • Projects evaluation
2.2	Differentiate between Symmetric and Asymmetric Encryption	<ul style="list-style-type: none"> • Lectures • Problem solving cases 	<ul style="list-style-type: none"> • Homework assignments • Examinations • Presentations
3.0	Interpersonal Skills & Responsibility		

3.1	Ability to relate to, and collaborate effectively with peer groups.	<ul style="list-style-type: none"> • Problem solving cases • Group Work • Writing reports 	<ul style="list-style-type: none"> • Evaluation of individual work (assignments and reports) • Presentation by the students
3.2	Have self-management capabilities to meet deadlines	<ul style="list-style-type: none"> • Problem solving cases • Group Work • Writing reports 	<ul style="list-style-type: none"> • Evaluation of individual work (assignments and reports) • Presentation by the students
4.0	Communication, Information Technology, Numerical		
4.1	Use protection methods and technologies	<ul style="list-style-type: none"> • lectures to outline the utilization of available protection technologies • Problem solving cases • Independent study (project) 	<ul style="list-style-type: none"> • Examinations and homework assignments • Presentations.
5.0	Psychomotor		
5.1			
5.2			

5. Map course LOs with the program LOs. (Place course LO #s in the left column and program LO #s across the top.)

Course LOs #	Program Learning Outcomes (Use Program LO Code #s provided in the Program Specifications)								
	1.1	1.2	1.3	2.1	2.2	3.1	3.2	4.1	4.2
1.1	X	-	-	-	-	-	-	-	-
1.2	-	X	-	-	-	-	-	-	-
2.1	-	-	-	X	-	-	-	-	-
2.2	-	-	-	-	-	-	-	-	-
2.3	-	-	-	-	X	-	-	-	-
3.1	-	-	-	-	-	-	X	-	-
4.1	-	-	-	-	-	-	-	X	-

6. Schedule of Assessment Tasks for Students During the Semester

	Assessment task (e.g. essay, test, group project, examination, speech, oral presentation, etc.)	Week Due	Proportion of Total Assessment
1	Quiz1	4	10

2	Mid Exam	8	20
3	Assignments / Participation/ Attendance	Continuous	20
4	Quiz 2	12	10
5	Final	16	40

D. Student Academic Counseling and Support

1. Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice. (include amount of time teaching staff are expected to be available each week)

Five office hours weekly by the faculty for individual counseling and guidance

E. Learning Resources

1. List Required Textbooks

“Corporate Computer Security”, 4/e Randall J. Boyle • Raymond R. Panko, 2014, Prentice Hall; ASIN: B011DAZR4Y

2. List Essential References Materials (Journals, Reports, etc.)

<http://www.springer.com/computer/security+and+cryptology/journal/10207>

3. List Recommended Textbooks and Reference Material (Journals, Reports, etc)

Information Security: The Complete Reference, Second Edition by Mark Rhodes-Ousley

4. List Electronic Materials, Web Sites, Facebook, Twitter, etc.

<http://www.amazon.com/Information-Security-Complete-Reference-Edition/dp/0071784357>

5. Other learning material such as computer-based programs/CD, professional standards or regulations and software.

http://download.cnet.com/windows/bloodshed-software/3260-20_4-59072-1.html

<http://learncryptography.com/>

F. Facilities Required

Indicate requirements for the course including size of classrooms and laboratories (i.e. number of seats in classrooms and laboratories, extent of computer access etc.)
1. Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.) Class room demonstration rooms/labs
2. Computing resources (AV, data show, Smart Board, software, etc.) Data show projector
3. Other resources (specify, e.g. if specific laboratory equipment is required, list requirements or attach list)

G. Course Evaluation and Improvement Processes

1 Strategies for Obtaining Student Feedback on Effectiveness of Teaching <ul style="list-style-type: none">• Course Evaluation Form.• Course learning outcome survey
2 Other Strategies for Evaluation of Teaching by the Instructor or by the Department Faculty visit and evaluation
3 Processes for Improvement of Teaching

Students and faculty feedback
4. Processes for Verifying Standards of Student Achievement (e.g. check marking by an independent member teaching staff of a sample of student work, periodic exchange and remarking of tests or a sample of assignments with staff at another institution)
5 Describe the planning arrangements for periodically reviewing course effectiveness and planning for improvement.

Name of Instructor: _____

Signature: _____ Date Report Completed: _____

Name of Field Experience Teaching Staff: _____

Program Coordinator: _____

Signature: _____ Date Received: _____