Course Specifications

Institution:	College of Science at Az Zulfi
Academic Department :	Computer Science and Information
Programme :	Computer Science and Information
Course :	Information Security
Course Coordinator :	
Programme Coordinator :	Assoc. Prof. Y. Azzam
Course Specification Approved Date :	22/ 12 / 1435 H

A. Course Identification and General Information

1 - Course title : Information Security	Course Code: CSI - 447
2. Credit hours : 3 (2 lecture + 2 lab)	
3 - Program(s) in which the course is offered: Computer Science and Information	
4 – Course Language : English	
5 - Name of faculty member responsible for the course:	
6 - Level/year at which this course is offered : : 10th Level (Elective)	

6 - Level/year at which this course is offered : : 10th Level (Elective)

7 - Pre-requisites for this course (if any) :
- Cryptography and Information Security (CSI 423)

8 - Co-requisites for this course (if any) : N/A

9 - Location if not on main campus **:** College of Science at AzZulfi

10 - Mode of Instruction (mark all that apply)

A - Traditional classroom	√	What percentage?	80 %
B - Blended (traditional and online)	√	What percentage?	10 %
D - e-learning	√	What percentage?	10 %
E - Correspondence		What percentage?	……. %
F - Other		What percentage?	……. %

Comments :

B Objectives

What is the main purpose for this course?

This course is to make students familiar with the basic concepts of information systems security. The course aims to the security goals, security functions, and security mechanisms. The content is: Introduction to information security, information security and risk management, access control, security architecture and design, physical environmental security, telecommunications and network security, business continuity and disaster recovery, application security and operation security. The choice of appropriate encryption/decryption is the key in the development of efficient secure information system. In fact, it is difficult to create a trusted information system without a good understanding of a number of fundamental
information security issues. This module aims:

1. To learn how the choice of encryption and decryption algorithm design methods impacts the performance of any information system.
2. To learn how to define the security problems.
3. To study specific algorithms for encryption and decryption.
4. To study a wide spectrum of different issues where we can protect our information systems.

Briefly describe any plans for developing and improving the course that are being implemented :

5. Using group discussion.
6. Updating the materials of the course to cover the new topics of the field.
7. Increasing the ability of the students to implement the algorithms that are presented in the course.

C. Course Description

1. Topics to be Covered

List of Topics	No. of Weeks	Contact Hours
1. Introduction to information Security: History of information security, what is security? CNSS Security Model, Security systems development life cycles, security professionals and organization, the need for security, business needs first, threats, attacks, secure software developments, legal, ethical and professional issues in information security.	3	12
2. Information security and risk management: an overview of risk management, risk identification, risk assessment, risk control strategies, selecting a risk control strategy.	4	16
3. Security technology: access control, Firewalls, protecting remote connections, intrusion detection and prevention systems.	4	16
4. Physical environmental security: physical access control, fire security and safety, failure of supporting utilities, mobile and portable systems.	4	16

2. Course components (total contact hours and credits per semester):

	Lecture	Tutorial	Laboratory	Practical	Other:	Total
Contact Hours	30	-	30	-	-	60
Credit	30	-	15	-	-	45

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

5 Hours

The private self-study of the attending student is crucial for this course. It includes:
- reading carefully the topics in the textbook or reference book,
- implementing security algorithms using C++ ,
- browsing the websites that concerned with the course,
- solving the exercises that are assigned in each chapter,
- discussing the course topics with the instructor in his office hours,

The total workload of the student in this course is then: 60 + 5 x 15 = 135 work hours

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

	NQF Learning Domains And Course Learning Outcomes	Course Teaching Strategies	Course Assessment Methods
1.0	**Knowledge**		
1.1	Explain the objectives of information security.	Lectures. Lab demonstrations. Case studies. Individual presentations.	Written Exam Homework assignments Lab assignments Class Activities Quizzes
1.2	Discuss the importance and applications of each of confidentiality, integrity, and availability.		
1.3	Understand the basic categories of threats to computers and networks.		
2.0	**Cognitive Skills**		
2.1	Analyze issues for creating security policy for a large	Small group	Written Exam

	NQF Learning Domains And Course Learning Outcomes	Course Teaching Strategies	Course Assessment Methods
2.2	organization. Defend the need for protection and security, and the role of ethical considerations in computer use.	discussions. Whole group discussions. Brainstorming. Presentations.	Homework assignments Lab assignments Class Activities Quizzes
3.0	**Interpersonal Skills & Responsibility**		
3.1	Present issues and solutions in appropriate form to communicate effectively with peers and clients from specialist and non-specialist backgrounds.	Small group discussions. Whole group discussions. Brainstorming. Presentations.	Written Exam Homework assignments Lab assignments Class Activities Quizzes
4.0	**Communication, Information Technology, Numerical**		
4.1	Analyze the local and global impact of information security on individuals, organizations, and society	Small group discussions. Whole group discussions. Brainstorming. Presentations.	Observations Homework assignments Lab assignments Class Activities
4.2	function effectively on teams to accomplish a common goal.		
5.0	**Psychomotor**		
5.1	....	....	....

5. Schedule of Assessment Tasks for Students During the Semester:

	Assessment task	Week Due	Proportion of Total Assessment
1	First written mid-term exam	6	15%
2	Second written mid-term exam	12	15%
3	Presentation, class activities, and group discussion	Every week	10%
4	Homework assignments	After each chapter	10%
5	Implementation of presented protocols	Every two weeks	10%
6	Final written exam	16	40%
7	Total		100%

D. Student Academic Counseling and Support

Office hours: Sun: 10-12, Mon. 10-12, Wed. 10-12
Office call: Sun. 12-1 and Wed 12-1

Email: h.haly@mu.edu.sa
Mobile: 0538231332

E. Learning Resources

1. List Required Textbooks :   • Michael E. Whitman, Herbert J. Mattord, Principles of information security, Cengage Learning, 2013.
2. List Essential References Materials :   • W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, Six Edition. 2013.
3. List Recommended Textbooks and Reference Material :   • IEEE trans. Of Information Security.
4. List Electronic Materials :   • www.iacr.org
5. Other learning material :   • N/A

F. Facilities Required

1. Accommodation   • Classrooms and Labs as that available at college of science at AzZulfi are enough.
2. Computing resources   • Smart Board
3. Other resources   • N/A

G   Course Evaluation and Improvement Processes

1 Strategies for Obtaining Student Feedback on Effectiveness of Teaching: • Questionnaires (course evaluation) achieved by the students and it is electronically organized by the university.   • Student-faculty management meetings.
2 Other Strategies for Evaluation of Teaching by the Program/Department Instructor :   • Discussion within the staff members teaching the course   • Departmental internal review of the course.

3 Processes for Improvement of Teaching :
  • Periodical departmental revision of methods of teaching.
  • Monitoring of teaching activates by senior faculty members.
  • Training course.

4. Processes for Verifying Standards of Student Achievement
  • Reviewing the final exam questions and a sample of the answers of the students by others.
  • Visiting the other institutions that introduce the same course one time per semester.
  • Watching the videos of other courses by international institutions.

5 Describe the planning arrangements for periodically reviewing course effectiveness and planning for improvement :
  • Course evaluation
  • Exam evaluation
  • Improvement plan

Course Specification Approved
Department Official Meeting No (6) Date 22 / 12 / 1435 *H*

Course's Coordinator

Name : ....

Signature : ....

Date : ..../ ... / ...... *H*

Department Head

Name :   Dr. Yosry Azzam

Signature :   ....

Date :   22/12 / 1435 *H*