Kingdom of Saudi Arabia

The National Commission for Academic Accreditation & Assessment

Computing Department, Community College Dammam
University of Dammam

Course Specifications
(CS)

Information Security

IT310

Information Security

Course Specifications

Institution: University of Dammam	**Date of Report**
College/Department: Dammam-Community College / Computer Science Department	

A. Course Identification and General Information

1. Course title and code: Information Security (IT310)
2. Credit hours: 3 (3 Theoretical)
3. Program(s) in which the course is offered.
(If general elective available in many programs indicate this rather than list programs)
Information systems and Information technology tracks
4. Name of faculty member responsible for the course
5. Level/year at which this course is offered: 2nd Level - Year 1
6. Pre-requisites for this course (if any): CS120
7. Co-requisites for this course (if any):
8. Location if not on main campus
9. Mode of Instruction (mark all that apply)

a. Traditional classroom	√	What percentage?	%80
b. Blended (traditional and online)		What percentage?	
c. e-learning	√	What percentage?	%20
d. Correspondence		What percentage?	
f. Other		What percentage?	

Comments:

B Objectives

1. What is the main purpose for this course? 1. To be familiar with computing systems security and their significance. 2. To be familiar with the division of computer systems in terms of security requirements. 3. To know the digital systems interference methods. 4. To be able to measure computer systems performance and making sure that they have not been breached. 5. To be familiar with military and navigational systems, 6. To be able to protect software and information against potential threats. 7. To be able to determine the requirements of computer systems. 8. To know the environmental and external threats to computer systems.
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)

C. Course Description (Note: General description in the form to be used for the Bulletin or handbook should be attached)

This course aims to introduce to the students the fundamental basics of Computer Security Systems and the potential risks, and Vulnerabilities in these systems.

1. Topics to be Covered

List of Topics	No. of Weeks	Contact Hours
1. Introduction to computing systems security.	1	3T
2. Potential threats, risks and breaches.	1	3T
3. Preventing unauthorized access by third parties.	1	3T
4. Networks security.	2	6T
5. Reliable security systems.	2	6T
6. Distributed security systems.	2	6T
7. Internet security systems.	2	6T
8. Security system management.	2	6T
9. Security requirements.	1	3T
10. Future trends in information systems security.	1	3T

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

	Lecture	Tutorial	Laboratory	Practical	Other:	Total
Contact Hours	45					45
Credit	45					45

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

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	Demonstrate an understanding of the core concepts of information security and encryption systems.	Lecture-Discussion, Presentations ,Problem-solving	Recitations, assignments, seatwork , and major exam
1.2	Identify and explain the vulnerabilities of information system as well mitigations to information system attacks.		
2.0	**Cognitive Skills**		
2.1	Use appropriate tools and techniques for IS security.	Lecture-Discussion, Presentations, Problem-solving, Simulation, and group activity	Recitations, Seatwork, Project/ Case Study, and major exam
2.2	Implement Operating System (OS) hardening practices and procedures to achieve workstation and server security		
3.0	**Interpersonal Skills & Responsibility**		
3.1	Analyze common threats and the access control mechanism used for user authentication and authorization	Lecture-Discussion, Presentations ,Problem-solving	Recitations, assignments, seatwork , and major exam
3.2	Analyze the use of cryptographic and securing Internet Protocol (IP) communications by using Internet Protocol Security (IPSec);		
4.0	**Communication, Information Technology, Numerical**		
4.1	Articulate industry trends in the particular domains	Group activity	Project/ Case Study
4.2	Work effectively as part of a team		
5.0	**Psychomotor**		
5.1	**N/A**	**N/A**	**N/A**
5.2			

5. Course Learning Outcomes Mapping Matrix Identify on the table below the Course Outcomes and Relationship to PLOs	
Course Learning Outcomes	**Program Learning Outcomes**
1. Knowledge	
1.1	**1.1**
1.2	**1.2**
2. Cognitive skills	
2.1	**2.3**
2.2	**2.1 , 2.2**
3. Interpersonal Skills and responsibility	
3.1	**3.1, 3.2**
3.2	**3.3**
4. Communication IT and Numeral Skills	
4.1	**4.2, 4.3**
4.2	**4.1**
5. Psychomotor Skills	
5.1	**N/A**

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	First quiz	4	%5
2	Mid term	8	%20
3	Second quiz	10	%5
4	Project	13	%20
5	Attendance/Participation	All weeks	%10
6	Final	17	%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) • Each group of students is assigned to a member of staff who will be available for help and academic guidance office hours at specific 2 hours on daily basis.

E. Learning Resources

1. List Required Textbooks • Michael E. Whitman and Herbert J. Mattord " Management of Information Security", Course Technology; 3rd edition (January 19, 2010) ISBN-10: 1435488849 , ISBN-13: 978-1435488847.
2. List Essential References Materials (Journals, Reports, etc.) • Charles P. Pfleeger and Shari Lawrence Pfleeger , Security in Computing 4th Edition, 2006, Prentice Hall, ISBN 978-0132390774.
3. List Recommended Textbooks and Reference Material (Journals, Reports, etc)
4. List Electronic Materials (eg. Web Sites, Social Media, Blackboard, etc.) • Blackboard and Social Media
5. Other learning material such as computer-based programs/CD, professional standards or regulations and software. • CDs accompanied with the text book, power point lectures and essential references

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.) Classrooms: • Furnished with a large central table or multiple small tables that can be grouped into one central table • Designed for up to 25 students • Size the room allowing 1sq meter per seat
2. Computing resources (AV, data show, Smart Board, software, etc.) • Smart Board, projector, internet, and whiteboard**.**
3. Other resources (specify, e.g. if specific laboratory equipment is required, list requirements or attach list) • No

G. Course Evaluation and Improvement Processes

1 Strategies for Obtaining Student Feedback on Effectiveness of Teaching: • Student questionnaires to be assessed by independent body. • Assessment of course teaching strategies by independent body.
2 Other Strategies for Evaluation of Teaching by the Program/Department Instructor: • Student questionnaires to be assessed by department.
3 Processes for Improvement of Teaching: • Attending workshop, reading books, and the searching for e-resources. • Revision of course contents, course specifications, and strategies every 5 years.
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) • Check marking by an independent member of staff of a sample of student work. • Periodic exchange and remarking of a sample of assignments with a member of staff in another institution
5 Describe the planning arrangements for periodically reviewing course effectiveness and planning for improvement. • Reviewing student's feedback. • Update text books. • Consulting other top universities course specifications and contents.