



Course Specifications

Course Title:	Information Security Foundations
Course Code:	CYB 0101
Program:	Computer Science (Cybersecurity)
Department:	Applied Sciences
College:	Applied College
Institution:	Imam Muhammad Bin Saud Islamic University

Table of Contents

A. Course Identification	3
6. Mode of Instruction (mark all that apply)	3
B. Course Objectives and Learning Outcomes	3
1. Course Description	3
2. Course Main Objective	3
3. Course Learning Outcomes	4
C. Course Content	4
D. Teaching and Assessment	4
1. Alignment of Course Learning Outcomes with Teaching Strategies and Assessment Methods.....	4
2. Assessment Tasks for Students	6
E. Student Academic Counseling and Support	6
F. Learning Resources and Facilities	6
1. Learning Resources	6
2. Facilities Required	6
G. Course Quality Evaluation	7
H. Specification Approval Data	7

A. Course Identification

1. Credit hours:	3(2 theory , 2 lab)			
2. Course type				
a.	University <input type="checkbox"/>	College <input type="checkbox"/>	Department <input checked="" type="checkbox"/>	Others <input type="checkbox"/>
b.	Required <input checked="" type="checkbox"/>	Elective <input type="checkbox"/>		
3. Level/year at which this course is offered:	First Semester			
4. Pre-requisites for this course (if any):	None			
5. Co-requisites for this course (if any):	None			

6. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	3hours\week	100%
2	Blended		
3	E-learning		
4	Distance learning		
5	Other		

7. Contact Hours (based on academic semester)

No	Activity	Contact Hours
1	Lecture	20
2	Laboratory/Studio	20
3	Tutorial	
4	Others (specify)	
	Total	40

B. Course Objectives and Learning Outcomes

1. Course Description

This course covers the basics of information security, where the student will learn information security models, including achieving physical security of information, security of procedures and operations, control of access to information and methods of defense against various risks, including piracy and unauthorized access to electronic systems and others. This course also covers tools for protecting the confidentiality of information such as encryption, securing networks and the Internet, reducing the risks of virus attacks, and firewalls to reduce attacks. It also covers methods of protection to ensure the availability and integrity of information. Also this course will mention the risk management and the legal and ethical issues.

2. Course Main Objective

The course aims to train the student on the basics of information security and how to identify risks and methods of defense against these risks. This course aims to enhance the skill of information protection at its various levels and mechanisms of application.

3. Course Learning Outcomes

CLOs		Aligned PLOs
1	Knowledge and Understanding	
1.1	To understand different types of attacks and threatened systems, the access control, accuracy, and intrusiveness.	2ع,1ع
1.2	Demonstrate information security and its needs, and to understand information security implementations.	2ع
2	Skills :	
2.1	To examine cryptographic system, and to deal with Information Security Management.	2م,1م
2.2	To be able to analyze Legal, ethical, and professional to defend against vulnerabilities.	7م
2.3	To examine how key security technology deal with systems.	1م
3	Values:	
3.1	To implement information security system.	7م,3ق,2ق,1ق

C. Course Content

No	List of Topics	Contact Hours
1	Module1:Introduction to information Security	4
2	Module2:The need for information security	3
3	Module3:Information Security Management	4
4	Module5:Planning for Security	3
5	Module6:Legal, ethical, and professional issues in information security	4
6	Module8:Security technology; Access control, firewall, and VPNs	7
7	Module9:Security technology; Intrusion detection and prevention systems and other security tools	5
8	Module10:Cryprography	4
9	Module11:Implemeting Information Security	3
10	Module12:Information Security Maintenance	3
Total		40

D. Teaching and Assessment

1. Alignment of Course Learning Outcomes with Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
1.0	Knowledge and Understanding		
1.1	To understand different types of attacks and threatened systems, the access control, accuracy, and intrusiveness.	Class lectures Class Discussion Questions/Answers sessions in class Home work assignments Quizzes Case studies and Analysis.	Quizzes Homework and Assignments. Written exams (Midterm and final). Writing reports.

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
1.2	Demonstrate information security and its needs, and to understand information security implementations.	Class lectures Class Discussion Questions/Answers sessions in class Home work assignments Quizzes Case studies and Analysis.	Quizzes Homework and Assignments. Written exams (Midterm and final). Writing reports. Study cases.
2.0	Skills		
2.1	To examine cryptographic system, and to deal with Information Security Management.	Class lectures Class Discussion Questions/Answers sessions in class Home work assignments Quizzes Case studies and Analysis.	Quizzes Homework and Assignments. Written exams (Midterm and final). Writing reports. Study cases.
2.2	To be able to analyze Legal, ethical, and professional to defend against vulnerabilities.	Class lectures Class Discussion Questions/Answers sessions in class Home work assignments Quizzes Case studies and Analysis.	Quizzes Homework and Assignments. Written exams (Midterm and final). Writing reports. Study cases.
2.3	To examine how key security technology deal with systems.	Class lectures Class Discussion Questions/Answers sessions in class Home work assignments Quizzes Case studies and Analysis.	Quizzes Homework and Assignments. Written exams (Midterm and final). Writing reports. Study cases.
3.0	Values		
3.1	To implement information security system.	Class lectures Class Discussion Questions/Answers sessions in class Home work assignments Quizzes Case studies and Analysis.	Quizzes Homework and Assignments. Written exams (Midterm and final). Writing reports. Study cases.

2. Assessment Tasks for Students

#	Assessment task*	Week Due	Percentage of Total Assessment Score
1	Quizzes	Week3,5	10%
2	Midterm1	Week 6	15%
3	Midterm2	Week9	15%
4	Pass CISCO Networking Academy course	Week10	10%
5	Lab Evaluations	All Semester	10%
6	Final	Week13	40%

*Assessment task (i.e., written test, oral test, oral presentation, group project, essay, etc.)

E. Student Academic Counseling and Support

Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice :

6 office hours per week.
 3 hours of weekly meetings
 Contact through the LMS
 Communication/interact via e-mails with students

F. Learning Resources and Facilities

1. Learning Resources

Required Textbooks	Principles of Information Security, Michael E. Whitman, Herbert J. Mattord · 2021
Essential References Materials	Information Security principles and practice, marks stamp, 2d Edition, 2011. Information Security and IT Risk Management , Manish Agrawal, Wiley. CompTIA Security+ All-in-One Exam Guide, Authors: WM. Arthur Conklin, Gregory White, Chuck Cothren, Roger L.Davis, Dwayne Williams. 6th Edition.
Electronic Materials	Online resources will be provided during class lectures.
Other Learning Materials	N/A

2. Facilities Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	Lecture room with Smart board Lab with 25 Pcs
Technology Resources (AV, data show, Smart Board, software, etc.)	PC and WiFi Internet access within the class room

Item	Resources
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	N/A

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Effectiveness of teaching and assessment	Student	Indirect using course evaluation survey
Quality of learning resources	Student and Faculty	Indirect using course evaluation and faculty survey

Evaluation areas (e.g., Effectiveness of teaching and assessment, Extent of achievement of course learning outcomes, Quality of learning resources, etc.)

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

Assessment Methods (Direct, Indirect)

H. Specification Approval Data

Council / Committee	
Reference No.	
Date	