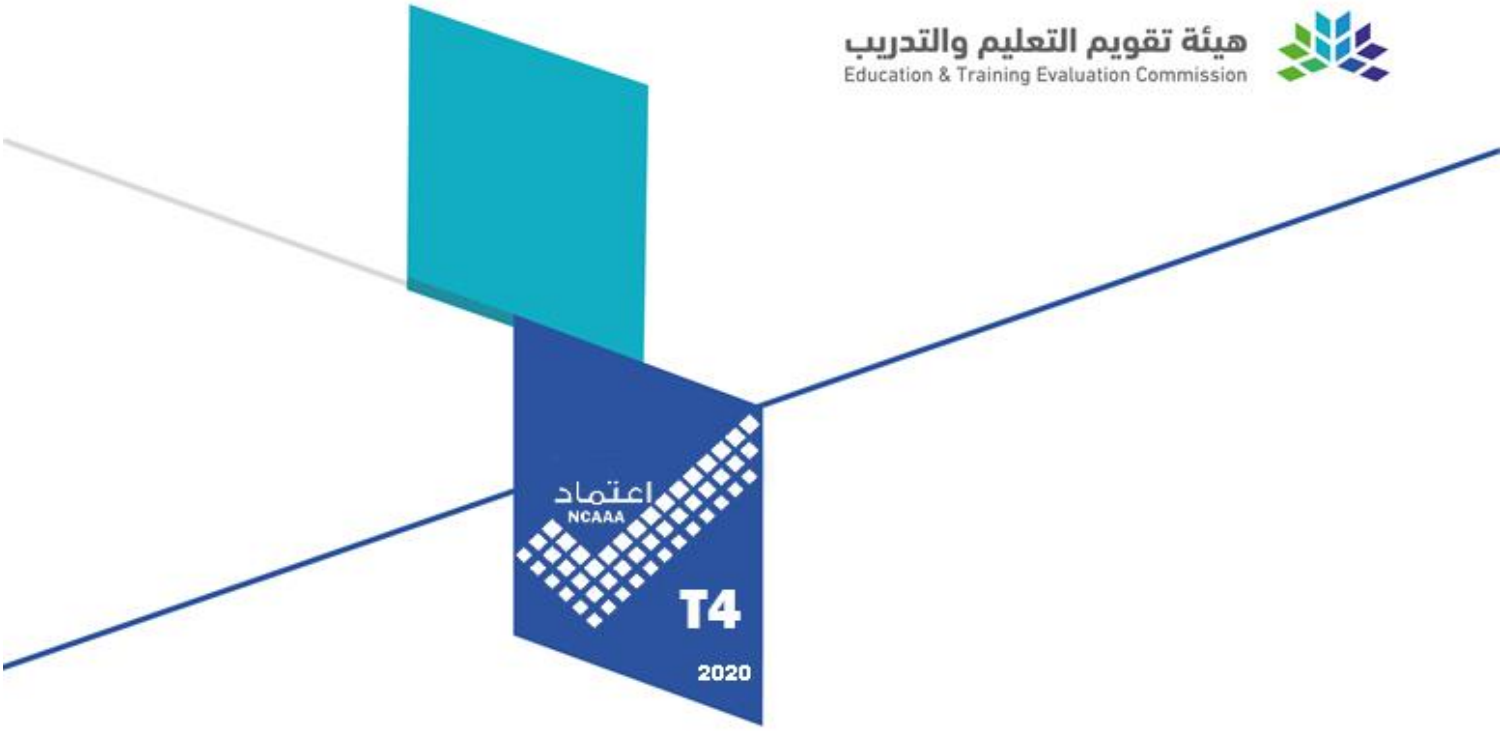
هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission



Course Specifications

Course Title:	Information Security
Course Code:	MIS 430
Program:	Management Information Systems
Department:	Management Information Systems
College:	College of Business Administration-Alkharj
Institution:	Prince Sattam bin Abdulaziz University

Table of Contents

A. Course Identification

1. Credit hours: 4
2. Course type **a.** University ☐ College ☐ Department ☑ Others ☐ **b.** Required ☑ Elective ☐
3. Level/year at which this course is offered: 11th level/ Fourth year
4. Pre-requisites for this course (if any)**:** MIS 201 – Management Information Systems
5. Co-requisites for this course (if any)**:**

6. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	**Traditional classroom**	48	100%
2	**Blended**		
3	**E-learning**		
4	**Distance learning**		
5	**Other**		

7. Contact Hours (based on academic semester)

No	Activity	Contact Hours
1	**Lecture**	48
2	**Laboratory/Studio**	
3	**Tutorial**	
4	**Others** (specify)	
	Total	48

B. Course Objectives and Learning Outcomes

1. Course Description

This course provides an introduction to the fundamental principles and topics of information security. Students will gain an understanding of the importance of security and its key concepts and terminologies. The course covers the threats posed to information security and common attacks associated with those threats, and the protection methods and technologies, including authentication, access control, encryption, and firewalls.

2. Course Main Objective

The main objective of this course is to provide students with the required knowledge in the field of information security, including the essential security concepts, threats, and protection mechanisms and technologies.

3. Course Learning Outcomes

CLOs		Aligned PLOs
1	**Knowledge and Understanding**	
1.1	Define key terms and concepts of information security	PLO1.1
1.2	Describe the approaches to information security implementation, and recognize the phases of the security systems development life cycle	PLO1.2 & PLO1.4
1.3	Identify the threats posed to information security and the more common attacks associated with those threats	PLO1.1
2	**Skills :**	
2.1	Demonstrate the ability to apply the commonly used methods and tools within the context of information security	PLO2.4
2.2	Use protection methods and technologies to investigate and provide solutions to information security problems	PLO2.3
2.3	Evaluate the capabilities and impacts of the most widely used protection technologies	PLO2.1
3	**Values:**	
3.1	Demonstrate capability to relate to and collaborate effectively with peer groups	PLO3.1 & PLO3.2

C. Course Content

No	List of Topics	Contact Hours
1	**Introduction to Information Security** Key Information Security Concepts, CIA Triad, Parkerian Hexad, Critical Characteristics of Information, CNSS Security Model, …	6
2	**Securing Components of Information systems** Software, Hardware, Data, People, Procedures, and Networks, …	4
3	**Approaches to Information Security Implementation** Bottom-up approach, top-down approach, security systems development life cycle (SecSDLC), …	4
4	**The Need for security** • Protecting the functionality of an organization, enabling the safe operation of applications, protecting data that organizations collect and use, safeguarding technology assets in organizations • Types of Threats: Acts of Human Error or Failure, Compromises to Intellectual Property, Deliberate Acts of Trespass, Deliberate Acts of Information Extortion, Deliberate Acts of Vandalism, Deliberate Acts of Theft,….	6
5	**Types of Attacks** Malicious Code, Virus Hoaxes, Brute Force Attack, Dictionary Attack, Denial-of-Service (DOS), Distributed Denial-of-Service (DDOS), Spoofing, Man-in-the-Middle, Spam, Social Engineering, …	6
6	**Risk Management** Risk Identification, Risk Assessment, Risk Control Strategies	5
7	**Protection Mechanisms & Technologies** Authentication, Access Control, Firewalls,…	6
8	**Cryptography** Basic Encryption Definitions, Substitution Cipher, Transposition Cipher, Symmetric Encryption, Asymmetric Encryption, RSA,…	5

9	**Implementing Information Security** Information security project management, technical aspects of implementation,…	3
10	**Security and Personal** Positioning and naming of the security function, Integrating solid information security concepts into personnel practices	3
Total		48

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	Define key terms and concepts of information security	• Lectures • Discussion-Based Teaching	• Homework assignments • In class short MCQs quizzes • Midterm exams • Final Exam
1.2	Describe the approaches to information security implementation, and recognize the phases of the security systems development life cycle	• Lectures • Problem solving cases	• Homework assignments • In class short MCQs quizzes • Midterm exams • Final Exam
1.3	Identify the threats posed to information security and the more common attacks associated with those threats	• Lectures • Problem solving cases • Independent study (project)	• Assignments • Examinations • Projects evaluation • Presentations evaluation
2.0	**Skills**		
2.1	Explain technical solutions used within the context of information security	• Lectures • Problem solving cases • Class discussions • Independent study (project)	• Assignments • Examinations • Projects evaluation • Presentations evaluation
2.2	Use protection methods and technologies to investigate and provide solutions to information security problems	• lectures • Problem solving cases • Independent study (project)	• Examinations • Projects evaluation • Presentations evaluation
2.3	Illustrate the capabilities of the most widely used protection technologies	• Lectures • Independent study (project)	• Assignments • Examinations • Projects evaluation
3.0	**Values**		
3.1	Demonstrate capability to relate to,	• Problem solving	• Projects evaluation

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
	and collaborate effectively with peer groups	cases • Group Work • Writing reports	• Presentations evaluation

2. Assessment Tasks for Students

#	Assessment task*	Week Due	Percentage of Total Assessment Score
1	Midterm exam1	5th	15%
2	Midterm exam 2	10th	15%
3	Quizzes	4th, 8th, and 10th	10%
4	Assignments	4th, 7th, and 9th	10%
5	Mini Projects	11th	10%
6	Final Examination		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 :
Office hours , 6 hr/ week

F. Learning Resources and Facilities

1.Learning Resources

Required Textbooks	Michael E. Whitman and Herbert J. Mattord, Principles of Information Security, 5th Edition, Course Technology, 2016.
Essential References Materials	1. William Stallings and Lawrie Brown, Computer Security: Principles and Practice, 4th edition, Pearson, 2017 2. Matt Bishop, Computer Security: Art and Science, 2nd edition, Addison-Wesley Professional, 2018 3. Wm. Arthur Conklin, Gregory B. White, Chuck Cothren, and Dwayne Williams, Principles of Computer Security: Security+ and Beyond, 3rd Edition, McGraw Hill Technology Education, 2011
Electronic Materials	eBook available at: https://www.cengagebrain.co.uk/shop/isbn/9781285448367
Other Learning Materials	Multimedia files associated with the topics of the text book

2. Facilities Required

Item	Resources

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	_ Lecture room that can accommodate at least 30 students for lectures and discussions
Technology Resources (AV, data show, Smart Board, software, etc.)	- Data show - Smart Board - Computer with internet connection
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	_

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Effectiveness of teaching and assessment	Students	Direct through a survey
Extent of achievement of course learning outcomes	Faculty member/Program Supervisor	Indirect through evaluating student marks
Quality of learning resources	Students	Direct through a survey
Self-Assessment	Faculty member	Direct through investigating the contents of the course report

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	Department Council
Reference No.	2
Date	SEP 2022