هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

T-104
2022

Course Specification

T-104
2022

Course Specification

Course Title: **Information System Security**	
Course Code: **2345 CIS**	
Program: **Information Systems**	
Department: **NA**	
College: **Applied College**	
Institution: **King Khalid University**	
Version: **1**	
Last Revision Date: **12 August 2023**	

Table of Contents:

A. General information about the course:

Course Identification

1. Credit hours:	3

2. Course type

a.	University ☐	College ☐	Department☐	Track☐	Others☒
b.	Required ☒	Elective☐			

3. Level/year at which this course is offered:	4th Level

4. Course general Description:

To secure information is a challenge and essential component of every information system. The course is intended to help students' fundamental and comprehensive understanding of information security. The technical content of the course gives a broad overview of essential concepts and methods for providing and evaluating security in information processing systems. The course is organized on the following themes.

5. Pre-requirements for this course (if any): 2343 CIS

6. Co- requirements for this course (if any):

7. Course Main Objective(s):

- Overview of Information systems security
- Overview of systems and network security
- Building a secure organization
- Cryptography primer
- Detecting/Preventing systems Intrusion
- Unix and Linux security
- Cloud computing security
- Security technology

1. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1.	Traditional classroom	64	100
2.	E-learning		
3.	Hybrid ● Traditional classroom ● E-learning		
4.	Distance learning		

2. Contact Hours (based on the academic semester)

No	Activity	Contact Hours
1.	Lectures	32
2.	Laboratory/Studio	32
3.	Field	
4.	Tutorial	
5.	Others (specify)	
	Total	64

B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
1.0	Knowledge and understanding			
1.1	Define Information Systems Security and its majors' components.	k1	Lectures + Lab	Exams, Assignments, Quizzes
1.2	Describe the basic principles and techniques to build a secure Information System. ه	k1	Lectures + Lab	Exams, Assignments, Quizzes
1.3	Recognize the importance of cryptographic algorithms used in security in the context of the overall information systems.	k2	Lectures + Lab	Exams, Assignments, Quizzes
2.0	Skills			
2.1	Explain basic security concepts as confidentiality, integrity, availability and threats.	s1	Lectures + Lab	Exams, Assignments, Quizzes
2.2	Identify the major types of threats in information systems and the associated attacks.	s2	Lectures, Lab, group discussion	Exams, Assignments, Quizzes
2.3	Explain the obstacles and challenges to build a secure Information System.	s3	Lectures, Lab, group discussion	Exams, Lab Assignments, Quizzes
2.4	Demonstrate and evaluate the operating systems and cloud computing security.	s4	Lectures, Lab, group discussion	Exams, Lab Assignments, Quizzes
3.0	Values, autonomy, and responsibility			
3.1	Detect and prevent systems intrusions.	v1	Lectures, Lab, Case Study	Exams, Assignments and presentation
3.2	Participate and communicate with other students about specific IS security cases.	v2	Presentations, Lab, Groupwork	Exams, Assignments and presentation

C. Course Content

No	List of Topics	Contact Hours
1	**Overview of Information Systems Security:** - Levels of Impacts - Examples of security Requirements system - Computer security challenges - Policies and mechanisms - The OSI Security Architecture - Model of network security	**5**
2	**Building a Secure Organization:** - Obstacles to Security - Computers are powerful and complex - Current trend is to share, not protect - Security isn't about hardware and software - Ten steps to building a secure organization - Preparing for the building of security control assessment	4
3	**Cryptography:** - What is cryptography? - What is encryption - Famous cryptographic devices - Algorithms & Keys - Symmetric & Asymmetric Algorithms - **Encryption Techniques** ▪ **Transposition Ciphers** → Spartan Scytale and transposition cipher with keyword ▪ **Substitution Cipher** → Caesar cipher, shift cipher, affine cipher, Hill cipher, shift cipher and Vigenère cipher ▪ **Product Cipher** → German ADFGVX cipher ▪ **DES (Data Encryption Standard)**	5
4	**Detecting System Intrusions** - Introduction to DSI - Security Objectives - 0day Attacks - Malware - Antivirus Software - Security Awareness Training - Network-Based Detection of Systems Intrusion	3
5	**Preventing System Intrusion:** - What is an Intrusion - Know your enemy: hackers versus crackers - Motives - The crackers' tools of the trade - Bots - Symptoms of intrusions - Security policies - Risk analysis (vulnerability testing , audits and recovery)	5

	- Tools of your trade (intrusion detection systems (idss), firewalls, intrusion prevention systems, access control systems, unified threat management. - Controlling user access - Content filtering technology - Virtual Private Networks	
6	**Linux & Unix security:** - Unix & security - Basic Unix security overview - Achieving Unix security - Protecting user accounts and strengthening authentication - Limiting superuser privileges - Securing local and network file systems - Network configuration - Improving the security of Linux and Unix systems	5
7	**Cloud computing security:** - Cloud computing essentials - Securing Cloud computing - Operate and configure cloud security - Deployment models (e.g., public, private, hybrid, community) - Service models (e.g., IaaS, PaaS and SaaS) - Virtualization (e.g., hypervisor) - Legal and regulatory concerns (e.g., privacy, surveillance, data ownership, jurisdiction, eDiscovery) - Data storage and transmission (e.g., archiving, recovery, resilience) - Third party/outsourcing requirements (e.g., SLA, data portability, data destruction, auditing) - Shared responsibility model	5
		32

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Quiz 1	4	5
2.	Midterm Exam 1	7	10
3.	Practical Assessment	1 to 16	30
4.	Midterm Exam 2	12	10
5.	Quiz 2	14	5
6.	Final Exam	After week 16	40

*Assessment Activities (i.e., Written test, oral test, oral presentation, group project, essay, etc.)

E. Learning Resources and Facilities

1. References and Learning Resources

Essential References	Security in computing by Charles p. Pflueger, 5th edition 2015
Supportive References	Computer and Information Security handbook by John R Vacca, 2 nd Edition Cloud Management and Security Hardcover – 1 August 2014 by Imad M. Abbadi Cryptography_and_Network_Security,fourth edition by William Stallings
Electronic Materials	https://www.sciencedirect.com/ https://www.cloudflare.com/learning/security https://www.tutorialspoint.com/computer_security
Other Learning Materials	

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	▪ Lecture Rooms with data show ▪ Laboratories
Technology equipment (projector, smart board, software)	Eclipse IDE for Java Developers VMware and Kali Linux Internet connection is required in all labs
Other equipment (depending on the nature of the specialty)	

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Students	Indirect
Effectiveness of students assessment	Course Teacher	Direct
Quality of learning resources	Program Supervisor, Quality Unit	Direct
The extent to which CLOs have been achieved	Course Teacher	Direct
Other	Course Teacher, Quality Unit	Direct

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

Assessment Methods (Direct, Indirect)

G. Specification Approval Data

COUNCIL /COMMITTEE	
REFERENCE NO.	
DATE	