



Course Specification

— (Bachelor)

Course Title: **E-Commerce Security**

Course Code: **IS1455**

Program: **Bachelor in Information Systems**

Department: **Information systems**

College: **College of Computer and Information Sciences**

Institution: **Imam Mohammad Ibn Saud Islamic University**

Version: **1**

Last Revision Date: **May 14th, 2026**

Approved: 24/08/2025



Table of Contents

A. General information about the course:	4
B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods	5
C. Course Content.....	7
D. Students Assessment Activities.....	7
E. Learning Resources and Facilities	7
F. Assessment of Course Quality	8
G. Specification Approval.....	8



A. General information about the course:

1. Course Identification

1. Credit hours: 3 credit hours (lectures:3)

3

2. Course type

- A. ☐ University ☐ College ☒ Department ☐ Track ☐ Others
- B. ☒ Required ☐ Elective

3. Level/year at which this course is offered: Fourth Year

4. Course general Description:

This course introduces the fundamental concepts, technologies, tools, and practices used to secure electronic commerce systems and digital business environments. Students explore the security requirements of e-commerce platforms, including confidentiality, integrity, authentication, authorization, non-repudiation, privacy protection, and secure payment systems. The course covers cyber threats targeting e-commerce applications, web application vulnerabilities, cryptography, public key infrastructure (PKI), SSL/TLS protocols, digital signatures, firewalls, intrusion detection systems, risk management, and security policies. Students also study electronic payment systems, mobile commerce security, cloud security issues in e-commerce, consumer privacy concerns, legal and ethical aspects, business continuity planning, and emerging technologies related to secure online transactions. Practical case studies and security evaluation techniques are incorporated to provide students with hands-on understanding of securing e-commerce infrastructures.

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

IS1330 Fundamentals of Data Networks
IS1337 Application Development

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

7. Course Main Objective(s):

The main objective of this course is to equip students with the knowledge and practical understanding necessary to design, analyze, and manage secure e-commerce systems. Students will learn how to identify threats and vulnerabilities in online business environments, apply security technologies and protocols, evaluate secure electronic payment systems, and implement effective risk management and privacy protection strategies for electronic commerce applications.

2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	3 hours/week	100%





No	Mode of Instruction	Contact Hours	Percentage
2	E-learning		
3	Hybrid - Traditional classroom - E-learning		
4	Distance learning		

3. Contact Hours (based on the academic semester)

No	Activity	Contact Hours
1.	Lectures	45
2.	Laboratory/Studio	Not Applicable
3.	Field	Not Applicable
4.	Tutorial	Not Applicable
5.	Others (specify)	Not Applicable
Total		45

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	Explain the fundamental concepts, principles, and importance of e-commerce security in digital business environments.	K1(P)	Class Lectures	Quiz 1, Quiz 2, Midterm, Final
1.2	Describe common threats, attacks, vulnerabilities, and risks affecting e-commerce systems and online transactions.	K2(I)	Class Lectures, Self-learning, Discussions	Midterm, Final
1.3	Demonstrate understanding of	K3(I)	Class Lectures, Self-learning	Final



Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
	cryptography, authentication mechanisms, PKI, SSL/TLS, and digital certificates used in e-commerce security.			
2.0	Skills			
2.1	Analyze security requirements and evaluate risks associated with e-commerce platforms and applications.	<i>S1(P), S2(P)</i>	<i>Class Lectures, Case studies</i>	<i>Assignment 1, Assignment 2</i>
2.2	Apply security technologies and techniques to secure electronic payment systems, web applications, and online communication channels.	<i>S3(P)</i>	<i>Class Lectures, Discussions</i>	<i>Assignment 2, Project (Report)</i>
2.3	Assess security incidents and recommend appropriate countermeasures and security policies for e-commerce organizations.	<i>S4(I)</i>	<i>Class Lectures, Discussions</i>	<i>Project (Report)</i>
3.0	Values, autonomy, and responsibility			
3.1	Work effectively in teams to analyze and solve e-commerce security problems.	<i>V1(I)</i>	<i>Class Discussion, Lecture</i>	<i>Project Presentation</i>
3.2	Communicate technical security concepts effectively in written and oral forms.	<i>V3(I)</i>	<i>Lecture</i>	<i>Project Presentation</i>
...				

C. Course Content

No	List of Topics	Contact Hours
1.	Introduction to E-Commerce and E-Commerce Security	3
2.	E-Commerce Infrastructure and Security Requirements	3
3	Information Security Fundamentals and Risk Management	3
4	Threats, Vulnerabilities, and Cyber Attacks in E-Commerce	4
5	Cryptography Fundamentals and Encryption Techniques	4
6	Public Key Infrastructure (PKI), Digital Certificates, and Digital Signatures	3
7	Authentication, Authorization, and Access Control Mechanisms	3
8	Secure Communication Protocols (SSL/TLS, HTTPS)	3
9	Web Application Security and Secure Web Design	4
10	Electronic Payment Systems and Payment Card Security	4
11	Mobile Commerce and Cloud Security Issues	3
12	Firewalls, Intrusion Detection Systems, and Network Security	3
13	Privacy Protection, Legal, Ethical, and Compliance Issues	3
14	Business Continuity, Incident Response, Emerging Trends, and Project Discussions	2
Total		45

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Quiz	4,11	10%
2.	Midterm Exam	8	20%
3.	Assignment	7	10%
4	Group Project	15	20%
5	Final Exam	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	Kenneth C. Laudon and Carol Guercio Traver, <i>E-Commerce 2023–2024: Business, Technology, Society</i> , 18th Edition, Pearson.
Supportive References	William Stallings, <i>Cryptography and Network Security: Principles and Practice</i> , Pearson.
Electronic Materials	N/A





Other Learning Materials N/A

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	1. At least 30 seats 2. A projector connected to a PC preferably with Internet connection 3. Sliding board
Technology equipment (projector, smart board, software)	
Other equipment (depending on the nature of the specialty)	N/A

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Students	Indirect using course evaluation survey
Effectiveness of Students assessment	Faculty members	Direct method using TOS file
Quality of learning resources	Students and Faculty	Indirect using course evaluation survey and faculty survey
The extent to which CLOs have been achieved	Faculty members	Direct method using TOS file
Other		

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

Assessment Methods (Direct, Indirect)

G. Specification Approval

COUNCIL /COMMITTEE	IS CURRICULUM APPROVAL & DEVELOPMENT COMMITTEE IS QAC / / IS COUNCIL
REFERENCE NO.	
DATE	

