هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

T-104
2022

Course Specification

Course Title:	**Information Systems Security**
Course Code:	**IS1512**
Program:	**Computer Information Systems**
Department:	**Computer Information Systems**
College:	**Computer Science & Information Technology**
Institution:	**Al-Baha University**
Version:	**1**
Last Revision Date:	**March 29, 2023**

Table of Contents:

A. General information about the course:

Course Identification					
1. Credit hours:	3 Credit Hours (3, 0, 0) (Lecture, Lab, Tutorial) (3 Contact Hours)				
2. Course type					
a.	University ☐	College ☐	Department☒	Track☐	Others☐
b.	Required ☒	Elective☐			
3. Level/year at which this course is offered:	9th Level/3rd Year				
4. Course general Description This module is designed to provide students with a comprehensive understanding of information systems security principles, practices, and technologies. The course will explore different aspects of information security, including threats, vulnerabilities, risk management, access control, authentication, and authorization. Students will learn about different types of attacks, such as social engineering, malware, and denial-of-service attacks, and the countermeasures that can be used to mitigate them. The module will also cover security policies, procedures, and best practices, as well as legal, ethical, and social issues related to information security.					
5. Pre-requirements for this course (if any): IS1002 – Foundations of Information Systems					
6. Co- requirements for this course (if any): None					
7. Course Main Objective(s) 1. Understand the principles and concepts of information systems security. 2. Identify the different types of threats and vulnerabilities that exist in information systems. 3. Analyze and assess the risks associated with information systems security. 4. Evaluate different security measures, technologies, and techniques used to protect information systems. 5. Understand the importance of access control, authentication, and authorization in information systems security. 6. Evaluate and apply security policies, procedures, and best practices in information systems. 7. Identify and analyze legal, ethical, and social issues related to information systems security. 8. Understand and analyze different types of attacks, including social engineering, malware, and denial-of-service attacks. 9. Evaluate and implement countermeasures and mitigation techniques to prevent and respond to security breaches and attacks. 10. Develop effective communication and collaboration skills to work as part of a team in addressing information systems security challenges.					

1. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1.	Traditional classroom	30	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	30
2.	Laboratory/Studio	
3.	Field	
4.	Tutorial	
5.	Others (specify)	
	Total	30

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	Describe the principles and concepts of information systems security.	K1	- Lectures - In-class discussions	- Midterm
1.2	Identify and explain the different types of threats, vulnerabilities, and attacks in information systems.	K2	- Lectures - In-class discussions	- Midterm
1.3	Evaluate and compare different security measures, technologies, and techniques used to protect information systems.	K3	- Lectures - Group projects - Case studies	- Midterm
1.4	Explain the importance of access control, authentication, and authorization in information systems security.	K3	- Lectures - Group projects - Case studies	- Assignments
1.5	Evaluate and apply security policies, procedures, and best practices in information systems.	K3	- Lectures - Group projects - Case studies	- Assignments
2.0	Skills			
2.1	Apply risk assessment techniques and develop security measures to protect information systems.	S1	- Lectures - Case studies	- Group-projects
2.2	Implement access control, authentication, and authorization mechanisms in information systems.	S2	- Lectures - Case studies	- Group-projects
2.3	Design and apply security policies, procedures, and best practices in information systems.	S3	- Lectures - Case studies	- Group-projects
3.0	Values, autonomy, and responsibility			
3.1	Recognize the importance of ethical and professional conduct in information systems security.	V1	- In-class discussions - Case studies	- Assignments
3.2	Take responsibility for maintaining the confidentiality, integrity, and availability of information systems.	V2	- In-class discussions - Case studies	- Assignments
3.3	Demonstrate the ability to work in-groups/independently and take initiative in addressing information systems security challenges.	V2	- Group projects	- Group-projects

Note: The Course Exit Survey will be used as an indirect Assessment Tool to evaluate the CLO.

C. Course Content

No	List of Topics	Contact Hours
1	Introduction to Information Systems Security: principles, concepts, and terminology.	2
2	Threats, Vulnerabilities, and Attacks: different types of attacks and their impact on information systems security.	4
3	Risk Assessment: techniques and methodologies for identifying and assessing information security risks.	4
4	Access Control, Authentication, and Authorization: concepts, mechanisms, and techniques for controlling access to information systems.	4
5	Malware: different types of malware, their characteristics, and how to detect and prevent them.	4
6	Security Policies and Procedures: design, implementation, and evaluation of security policies, procedures, and best practices for information systems security.	4
7	Security Audits and Testing: techniques and methodologies for auditing and testing the effectiveness of security measures.	4
8	Incident Response and Disaster Recovery: strategies and plans for responding to security incidents and recovering from disasters.	4
Total		30

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Assignment: (Risk Assessment)	3	10%
2.	Midterm	5	15%
3.	Group project	8	15%
4.	Final Exam	12	60%

*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	• Anderson, R. (2020). *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons. • Vacca, J. R. (2020). Computer and Information Security Handbook (3rd ed.). Morgan Kaufmann.
Supportive References	• Andress, J. (2014). *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress. • Goodrich, M. T., & Tamassia, R. (2011). *Introduction to computer security*. London, UK: Pearson. • Stamp, M. (2011). *Information security: principles and practice*. John Wiley & Sons. • ISO/IEC 27001:2013 Information security management systems. (2013). International Organization for Standardization. https://www.iso.org/standard/54534.html
Electronic Materials	• OWASP (Open Web Application Security Project). (n.d.). Top Ten Web Application Security Risks. https://owasp.org/Top10/ • SANS Institute. (n.d.). Information Security Resources. https://www.sans.org/security-resources/ • US-CERT (United States Computer Emergency Readiness Team). (2022). Cybersecurity and Infrastructure Security Agency. https://www.us-cert.gov/
Other Learning Materials	• Saudi Digital Library (SDL).

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	A classroom or lecture hall with a whiteboard for 25 students.
Technology equipment (projector, smart board, software)	• A digital image projection system with a connection to a desktop computer and laptop computer. • High-speed Internet connection. • An instructor computer station.
Other equipment (Depending on the nature of the specialty)	None

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	• Students • Faculty • Course Coordinator	• Surveys (indirect). • Direct feedback from students. Comprehensive Course report (where we can find information about teaching difficulties and action plan, …)
Effectiveness of students assessment	• Students • Faculty • Exam Evaluation Committee • Course Coordinator	• Surveys (indirect). • Direct feedback from students. Exam evaluation by the Exam Evaluation Committee (indirect)
Quality of learning resources	• Students • Faculty • Course Coordinator	• Surveys (indirect) Comprehensive Course report (where we can find information about difficulties and challenges about learning resources as well as consequences and action plan, …)
The extent to which CLOs have been achieved	• Faculty • Program Leader • Course Coordinator	• Student Results (direct) Comprehensive Course report (where we can find the CLO assessment results)
Other		

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

Assessment Methods (Direct, Indirect)

G. Specification Approval Data

COUNCIL /COMMITTEE	Curriculum Committee Meeting
REFERENCE NO.	
DATE	March 30, 2023