الجامعة الأهلية
AHLIA UNIVERSITY
BAHRAIN

COLLEGE OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION TECHNOLOGY
COURSE SYLLABUS/ SPECIFICATION

Course Code & Title: ITCS 404- Information Security Engineering

Weight: (2- 2 - 3)

Prerequisite: ITCS 327

NQF Level Allocated: 8

NQF Notional Hours / Credits: 120 notional hours/ 12 NQF credit

Description:

This course is to cover technical and administrative aspects of Information Security and Assurance. Topics covered: Information Security Concepts, The Need for Security, Security Services and Mechanisms, Security System Development, and Security Mechanisms, such as: Cryptographic systems, Information Hiding, Entity Authentication, and Digital Signature.

Objective:

1. To critically understand the specialist theories, standards, and concepts of information security.
2. To understand the phases needed to develop security systems.
3. To understand the business needs for security.
4. To critically evaluate different security techniques for providing different security services.
5. Research on new trends in information security.

Semester:

Instructor (s):

Office Telephone: **Email (s):**

Intended Learning Outcomes (ILOs):

A. Knowledge and Understanding	**NQF Level**
A1. Concepts and Theories: Demonstrate critical understanding of principles, standards, and concepts related to information security goals, mechanisms, and development.	Knowledge: theoretical understanding [Level 8]
A2. Contemporary Trends, Problems and Research: Demonstrate critical understanding of major current issues of information security, and research on new trends in protecting information.	Knowledge: theoretical understanding [Level 8]
A3. Professional Responsibility: N/A	N/A
B. Subject-Specific Skills	**NQF Level**
B1. Problem Solving: Critically analyze, assess, and identify the information security risks, vulnerabilities, threats, and possible attacks, as well as critically choose the appropriate security mechanisms to control security risks.	Knowledge: Practical Application [Level 8] Skills: Communication, ICT & Numeracy [Level 8]
B2. Modeling and Design: Design effective security systems to meet user requirements and to control information security risks of information systems.	Knowledge: Practical Application [Level 8]
B3. Application of Methods and Tools: Apply IT tools to implement different kinds of security techniques needed to protect information.	Knowledge: Practical Application [Level 8] Skills: Communication, ICT & Numeracy [Level 8]
C. Critical Thinking Skills	**NQF Level**
C1. Analytic: Critically assess, compare and select emerging and existing information security techniques, and analyze the security level of security systems.	Generic Problem Solving & Analytical skills [Level 8]
C2. Synthetic: Integrate appropriate information security components into one effective security system.	Generic Problem Solving & Analytical skills [Level 8]
C3. Creative: Demonstrate creativity in the development of effective security systems to control the problems of information systems.	Generic Problem Solving & Analytical skills [Level 8]
D. General and Transferable Skills	**NQF Level**
D1. Communication: Express and communicate complex ideas related to information security in written and oral forms.	Communication, ICT and Numeracy Skills [Level 8]
D2. Teamwork and Leadership: Demonstrate the ability to work as a group member/leader and share the ideas together.	Competence: Autonomy, Responsibility and Context [Level 8]
D3. Organizational and Developmental Skills: Demonstrate the ability to organize ideas and effectively allocate time in given assignments and project.	Competence: Autonomy, Responsibility and Context [Level 8]
D4. Ethical and Social Responsibility: Demonstrate an understanding of the role of culture as it applies to ethics in information security.	Competence: Autonomy, Responsibility and Context [Level 8]

Course Structure (Outline)

Course Structures						
Week	**Hours**		**ILOs**	**Unit/Module or Topic Title**	**Teaching Method**	**Assessment Method**
	Lec.	**Lab**				
1	2	2	A1	**Introduction to Information Security:** • Definitions. • Critical Information Characteristics. • Security Model. • SDLC Overview.	Lecture/Class Discussion	
2	2	2	A1	**The Business Need for Security:** • Threats. • Attacks.	Lecture/Class Discussion	
3	2	2	A1, D4	**Legal, Ethical, and Professional Issues in Information Security**	Lecture/ Debate/ Independent Learning	Case Study
4-5	4	4	A1, B1, B3	**Risk Management:** • Asset Identification and Valuation. • Threat Identification. • Vulnerability Identification. • Risk Identification and Assessment. **Lab:**Vulnerability Identification	Lecture/ Lab Demonstration/ In-Class Supervised Work	In-Lab Exercises/ Case Study
6	2	2	A1, A2, B2, D1, D3	**Risk Management:** Controlling Risk. **Lab:** Data Backup and Recovery	Lecture/ Lab Demonstration/ Independent Learning	Assignment 1/ In- Lab Exercises
7	2	2	A1, B2	**Logic Design**	Lecture/ In-Class Supervised Work	

8-10	6	6	A1, A2, B2, B3, C1, D1, D3	**Physical Design:** Cryptography and Cryptanalysis. **Lab:** Implementation of cryptographic systems and attacking methods.	Lecture/ In-Class Supervised Work/ Lab Demonstration/ In-Lab Supervised Work/ Independent Learning	Major Test (week 10)/ In-Class Exercises/ In-Lab Exercises/ Assignment 2
11-12	4	4	A1, A2, B2, B3, C1, D1, D3	**Physical Design:** Entity Authentication. **Lab:** Implementation of Entity Authentication techniques.	Lecture/ In-Class Supervised Work/ Lab Demonstration/ Independent Learning	In-Class Exercises/ In-Lab Exercises/ Assignment 3
13	2	2	A1, B2, B3, C1	**Physical Design:** Message Authentication. **Lab:** Implementation of Message Authentication techniques.	Lecture/ In-Class Supervised Work/ In-Lab Supervised Work	In-Class Exercises/ In-Lab Exercises
14	2	2	A1, B2, B3, C1	**Physical Design:** Information Hiding.	Lecture/ Lab Demonstration/ Class Discussion	
15	2	2	A2, B1, B2, B3, C1, C2, C3, D1,	Student Projects	Project Supervision	Evaluation of Project Presentations and Reports
16	2	-	A1, B1, B2, C1, C3, D4	All Topics		Final Exam

Teaching Materials:

Textbook(s):	1. Whitman M. and Mattord H. (2014) *Principles of Information Security,* 5th Edition, Delmar Cengage Learning. 2. Stallings W. (2016) *Cryptography and Network Security: Principles and Practice*, Global Edition, Pearson.
Handout(s):	Available on Moodle i.e. http://www.ahlia.edu.bh/moodle
Reference(s):	**1.** Tipton H. F. and Nozaki M. K. *Information Security Management Handbook*, 6th Edition, Auerbach Publications. 2. Schneier B. (2015) *Applied Cryptography: Protocols, Algorithms and Source Code in C*, 20th Anniversary Edition, John Wiley & Sons. 3. Katz J. and Lindell Y. (2014) *Introduction to Modern Cryptography*, 2nd Edition, Chapman and Hall. 4. Rhodes-Ousley M. (2013) *Information Security the Complete Reference*, 2nd Edition, McGraw Hill Professional. 5. Anderson R. J. (2010) *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd Edition, John Wiley & Sons. 6. Smith R. E. (2015) *Elementary Information Security*, 2nd Edition, Jones & Bartlett Learning. 7. Gibson D. (2014) *Managing Risk in Information Systems (Information Systems Security & Assurance)*, 2nd Edition, Jones & Bartlett Learning.

ASSESSMENTS:

Type of Assessment	Description	ILOs	Weighting
Exercises	Exercises, whether in-class or in-lab, cover problem solving and analysis questions and assess the students' ability in the analysis and application of different risk control techniques.	B1, B2, B3, C1	Formative
Case Studies	Different security project cases are analyzed and studied.	B1, D4	Formative
Assignments	Two assignments to be given to students. The assignments will assess students' skills in differentiating, and analyzing information security techniques in addition to literature review.	A2, B2, C1, D1, D3	20%

Major Test	The major test is a written, in-class 90 minutes test. It will cover topics studied in the first 10 weeks. The majority of the test's questions are problem solving, short answer, and analysis questions.	A1, B1, B2, C1, D4	20% 31/3/ 19
Project	Student will work as groups of 2-4 members to develop a security system as a project. This will go through several phases in which the student should analyze, and design a security system for a real world application.	A2, B1, B2, B3, C1, C2, C3, D1, D2, D3	20%
Final Exam	The final exam is a comprehensive, written exam and will be of two hours. It will consist of analysis, design, short-answer and essay questions.	A1, B1, B2, C1, C3, D4	40%
Overall			100%

Admissions	
Minimum number of students	**5**
Maximum number of students	**20**

Ahlia University values academic integrity. Therefore, all students must understand the meaning and consequences of cheating, plagiarism and other academic offences under the Code of Student Conduct and Disciplinary Procedures (see www.ahlia.edu.bh/integrity **for more information).**