Birzeit University
Computer Science Dept.

CSEC1310 ***Introduction to Cyber security and Proffesion ethics*** ***First semester 2022-2023***

==========

Lecturer:- Mr. Hafez Barghouthi (Office Masri321) hbargothi@birzeit.edu
Dr. Asem Kitana (Office Masri521) akitana@birzeit.edu

Text Book:-

Title：The basics of information security Understanding the Fundamentals of InfoSec in Theory and Practice (2nd edition)
Publisher :Elsiever
Author : Jason Andress

objectives:-

The basic aim of this course is to give a student brief introduction about different essential topics in information security and cyber security fields as following: Security aspects including Confidentiality, Privacy, Integrity, and Availability. Identification and authentication, Security Management, Access controls Models, Crypto bases, Network security bases, Intrusion detection and prevention Systems, Usable security. Computer crime ethics, hacking ethics, ethical/white hacking, confidentiality, accountability, ISSA Code of Ethics, and other professional code of ethics.

Learning Outcomes:

A) Knowledge and understanding

A1. Develop a thorough understanding of the theoretical and technical foundational knowledge in relevant domains including mathematics, networking, and computer science fundamentals.

A2. Develop a thorough understanding of the theoretical and technical foundational knowledge of cybersecurity and developing secure software.

A3. Develop comprehensive understanding of the theoretical and technical fundamental knowledge in information protection methods, and techniques for maintaining privacy and confidentiality.

A4. Develop critical knowledge and practical awareness of personal responsibility and professional codes of conduct in the context of cybersecurity and its ethical consideration.

B)Intellectuall/cognitive skills

B1. Analyze the concepts of cybersecurity and their implementation in developing secure software systems, for technical and professional use

B2. Analyze effectiveness of different information protection methods and techniques for maintaining privacy and confidentiality.

B3. Investigate the suitability of using alternative models and methods for developing secure software systems, for different application domains.

C)Subject specific and practical skills

C1. Apply cybersecurity foundational knowledge in the identification of cybersecurity requirements and the development of cybersecurity software solutions.

C.2. Apply different types of methods in assessing and analyzing security vulnerabilities, risks and threats associated with cyber systems.

D)General and transferable skills

D1. Able to communicate technical issues in an effective manner, both in written and oral format.

D2. Have critical thinking abilities to assess and analyze software engineering solutions, methods and approaches for the study and development of system.

D3. Have problem-solving skills to consider alternative approaches for different types of solutions in the context of cybersecurity systems.

D4. Have developed ethical professional skills to work within a team in a professional context of cybersecurity software development.

Support material:

- Text book: Cyber security essential, Authors: James Graham, Ryan Olson, Rick Howard, 1st edition, Auerbach Publications
- Text book:Security in computing, Authors: Shari Lawrence Pfleeger, Charles P. Pfleeger, Jonathan Margulies, 5th edition, Pearson
- Supplementary materials -All added articles to Ritaj.

Course Outline

Topics	*Chapters*
Security Terminology	1,3,4
Identification and Authentication	2
Cryptography	5
Network security	10
Midterm Exam	

Usable security	8 + Supplementary materials
Operating System security	11
Application Security	12
professional code of ethics.	6 + Supplementary materials

***Grading Policy*:-**

Midterm exam	25%
Quizzes	15%
Project and assignments	25 %
Final exam	35 %

No Make-Up Exams