The Hashemite University

الجامعـــــة الهاشميـــــة

Deanship of Academic Development and International Outreach

عمادة التطوير الأكاديمي والتواصل الدولي

Syllabus: Information Security (1910021711)

Second Semester 2021/2022

COURSE INFORMATION

Course Name: Information Security **Semester:** Second Semester 2021 /2022 **Department:** Department of CIS **Faculty:** Prince Al-Hussein bin Abdullah II Faculty for Information Technology	**Course Code:** 19110021711 **Section:** 3 **Core Curriculum**:
Day(s) and Time(s): Tuesday: 2-5 **Classroom:** IT: 210	**Credit Hours:** 3 **Prerequisites**: None

COURSE DESCRIPTION

This course is designed to cover issues of cyber and information security techniques and methodologies for detect and prevent attack, technical and non-technical aspects that affect the security and privacy of data. The course presents techniques used for illegal record linkage and background knowledge attacks, secure databases.

The course will introduce students Information Security Management issues of Information security, Risk Management, Computational Technologies for protecting privacy and while allowing society to collect and share person-specific data for many worthy purposes. The main topics include, introduction to cyber security, risk assessment, cyber security, privacy and anonymity models, data anonymization, privacy preserving data analytics, access control, secure computations, encryption, network Security, ethical hacking, and digital forensics. The foundations are drawn from a number of sub-disciplines of Computer Science including: database systems, computer security, cryptography, and statistics

Student are supposed to use some advanced techniques for masking databases, techniques to protect statistical databases, stenography techniques to protect the privacy of medical data. Finally, the course will introduce to some measures that are used for controlling the disclosure rate

in published databases including genetic data privacy, data privacy in distributed networks, data privacy in pervasive and cloud computing.

DELIVERY METHODS

The course will be delivered through a combination of active learning strategies. These will include:

- PowerPoint lectures and active classroom-based discussion
- Course Project
- E-learning resources: e-reading assignments through Model and Microsoft Team

FACULTY INFORMATION

Name	**Ala Said Mughaid**
Academic Title:	**Assistant Professor**
Office Location:	**IT 126**
Telephone Number:	**4404**
Email Address:	**Ala.mughaid@hu.edu.jo**
Office Hours:	**Sunday** 12.00-1.00 / **Tuesday** 2.00-3.00 *Please send an e-mail (ala.mughaid@hu.edu.jo) to meet at any other time.*

REFERENCES AND LEARNING RESOURCES

Required Textbook:

- Information Security Management Principles, David Alexander, Amanda Finch, David Sutton, Andy Taylor Andy Taylor (Author) 2013/ There is an new version in 2021

Suggested Additional Resources:

- E Introduction to Privacy-Preserving Data Publishing Concepts and Techniques, Benjamin C.M. Fung, Ke Wang, Ada Wai-Chee Fu, Philip S. Yu 2011
- Cyber Operations: Building, Defending, and Attacking Modern Computer Networks Raymond Chi-Wing Wong , Ada Fu 2019

Useful Web Resources:

https://www.unb.ca/cic/datasets/ids.html

https://www.kaggle.com/

COURSE OBJECTIVES

- Provide an overview of security models, hacking and digital forensics issues
- Provide introduction to Information Security and Risk Management
- Review advanced techniques to protect data privacy and privacy preserving data publishing
- Using modern techniques in data privacy protection
- Developing algorithms to maintain data security privacy many environments
- Overview of security countermeasures, access control, and network security measures

ACADEMIC SUPPORT

It is The Hashemite University policy to provide educational opportunities that ensure fair, appropriate and reasonable accommodation to students who have disabilities that may affect their ability to participate in course activities or meet course requirements. Students with disabilities are encouraged to contact their Instructor to ensure that their individual needs are met. The University through its Special Need section will exert all efforts to accommodate for individual's needs.

Special Needs Section:

Tel: 053903333 EXT 5023/4583

Location: (https://hu.edu.jo/facnew/index.aspx?typ=68&unitid=70000000)

Email: (huniv@hu.edu.jo)

COURSE REGULATIONS

Participation

Class participation and attendance are important elements of every student's learning experience at The Hashemite University, and the student is expected to attend all classes. A student should not miss more than 15% of the classes during a semester. *Those exceeding this limit of 15% will receive a failing grade regardless of their performance*. It is a student's responsibility to monitor the frequency of their own absences. **Attendance record begins on the first day of class irrespective of the period allotted to drop/add and late registration. It is a student's responsibility to sign-in; failure to do so will result in a non-attendance being recorded.**

In exceptional cases, the student, with the instructor's prior permission, could be exempted from attending a class provided that the number of such occasions does not exceed the limit allowed by the University. The instructor will determine the acceptability of an absence for being absent.

A student who misses more than 25% of classes and has a valid excuse for being absent will be allowed to withdraw from the course.

Plagiarism

Plagiarism is considered a serious academic offence and can result in your work losing marks or being failed. HU expects its students to adopt and abide by the highest standards of conduct in their interaction with their professors, peers, and the wider University community. As such, a student is expected not to engage in behaviours that compromise his/her own integrity as well as that of the Hashemite University.

Plagiarism includes the following examples and it applies to all student assignments or submitted work:

- **Use of the work, ideas, images or words of someone else without his/her permission or reference to them.**
- **Use of someone else's wording, name, phrase, sentence, paragraph or essay without using quotation marks.**
- **Misrepresentation of the sources that were used.**

The instructor has the right to fail the coursework or deduct marks where plagiarism is detected

Late or Missed Assignments

In all cases of assessment, students who fails to attend an exam, class project or deliver a presentation on the scheduled date without prior permission, and/or are unable to provide a medical note, will automatically receive a fail grade for this part of the assessment.

- Submitting a term paper on time is a key part of the assessment process. Students who fail to submit their work by the deadline specified will automatically receive a 10% penalty. Assignments handed in more than 24 hours late will receive a further 10% penalty. Each subsequent 24 hours will result in a further 10% penalty.
- In cases where a student misses an assessment on account of a medical reason or with prior permission; in line with University regulations an incomplete grade for the specific assessment will be awarded and an alternative assessment or extension can be arranged.

Student Complaints Policy

Students at Hashemite University have the right to pursue complaints related to faculty, staff, and other students. The nature of the complaints may be either academic or non-academic. For more information about the policy and processes related to this policy, you may refer to the students' handbook.

COURSE ASSESSMENT

Course Calendar and Assessment

Students will be graded through the following means of assessment and their final grade will be calculated from the forms of assessment as listed below with their grade weighting taken into account.

Assessment	Grade Weighting	Deadline Assessment
Midterm exam	30%	To be announced
Project	20%	To be announced
Presentations and Assignments	10%	Monthly
Final Exam	40%	To be announced

Description of Exams:

Test questions will predominately come from the material presented in the lectures. Semester exams will be conducted during the regularly scheduled lecture period. Exam will consist of a combination of multiple-choice, short answer, match, true and false and/or descriptive questions.

Homework:
Will be given for each chapter, while the chapter in progress you are supposed to work on them continuously and submit in next lecture when I finish the chapter.
You are also expected to work on in-chapter examples, self-tests and representative number of end of chapter problems. The answers of self-tests and end of chapter exercises are given at the end of the book.

Quizzes: Unannounced quizzes will be given during or/and at the end of each chapter based upon the previous lectures. It will enforce that you come prepared to the class.
No make-up exams, homework, or quizzes will be given. Only documented absences will be considered as per HU guidelines.

Grades are not negotiable and are awarded according to the following criteria*:

Letter Grade	Description	Grade Points
A+	Excellent	4.00
A		3.75
A−		3.50
B+	Very Good	3.25
B		3.00
B−		2.75
C+	Good	2.50
C	Fail	2.25

WEEKLY LECTURE SCHEDULE AND CONTENT DISTRIBUTION

Course Plan

Week no.	Topic	chapters
3	**Introduction:** • An introduction to Cyber Security and Risk Management • General Concepts in security • Security Models • Authentication • Authorization • Accounting • Threat • Risk • Assets, security measures • Assessing Security Risks • An introduction to data privacy • Information Security Management Principles • Information Risk • Physical and Environmental Security Controls	

Week no.	Topic	chapters
	• Disaster Recovery and Business Continuity Management	
2	**Security Countermeasures and Malicious Software** • General Controls • Physical Security • Technical Security • Procedural Security • Protection of Equipment • Processes to handle Intruder Alerts ○	
3	**Data privacy Modern techniques for data anonymization** • Privacy laws and regulations • An introduction to database protections systems • Methodological approaches to database protection • Differential privacy • Privacy Preserving data publishing • Multidimensional generalization • Generalization using condensation • Generalizing using synthetic data • Generalization using K-Anonymity • Perturbation and noise addition techniques • Preventing inference attacks • Types of attacks on anonymized data • Classification of database vulnerabilities • Measuring privacy risks in different communication media • Advanced statistical methods to anonymize data	
3	**Data Encryption** • Symmetric Encryption • Transposition Ciphers • Substitution Ciphers • Row Transposition Ciphers • Playfair Ciphers • Secure Multiparty Computation • Asymmetric Encryption • Public and Private Keys • Generator Numbers • RSA encryption • ElJamal Encryption	

Week no.	Topic	chapters
1	**Network security** • Internet Vulnerability • Port scanning • Spoofing • Denial of service • Firewalls • Intrusion detection Systems • Man in the Middle attacks • SYN Flooding attacks	
1	**Web and Database security techniques** • SQL Injection • Cross Site Scripting • Database privileges • Multilevel databases • Query modification • Social engineering and Phishing Attacks	
2	Project presentations	