جامعة فيلادلفيا  Philadelphia University	اسم النموذج: خطة تدريس مادة دراسية **Course Syllabus**	QFO-AP-FI-MO02
	الجهة المصدرة: كلية تكنولوجيا المعلومات	رقم الاصدار :1 Revision 1
	الجهة المدققة: عمادة التطوير والجودة	التاريخ :2017/11/05
		عدد صفحات النموذج: 3

Course Syllabus	
Course title: Information Security	**Course code:** 0750743
Course level: MSc	**Course prerequisite:** Computer networks
Lecture time: Wednesday, 16:00 – 19:00	**Credit hours:** 3

Academic Staff Specifics

Name	Rank	Office location	Office hours	e-mail address
Dr. Mohamed Bettaz	Prof.	Room 601 IT building	S, T, T 14:00-16:00 M, W, 15:00-16:00	mbettaz@philadelphia.edu.jo

Course description: This course addresses various topics, where the following are payed a special attention:

- Cyber stalking, fraud and abuse
- Denial of Service attacks
- Malware
- Techniques used by hackers
- Industrial espionage in cyberspace
- Encryption
- Computer security software
- Security policies
- Network scanning and vulnerability scanning

In this MSc course, theoretic study and investigations will be supplemented by research and programming projects related to various security subjects.

Teaching methods: Lectures, laboratories, seminars, workshops

Learning outcomes:

At the end of the module, you should be able to:

A. Knowledge and understanding

A1. Identify top threats to a computer network, and understand among other, viruses, Trojan horse, and DoS attacks

A2. Understand the basic methodology used by hackers, how spyware is used

A3. Explain the basics of encryption, and understand the function of protocols of VPNs

A4. Understand antispyware, recognize the importance of security policies, and understand how secure a system

A5. Understand basics of forensics principles

B. Intellectual skills

B1. Assess the likelihood of an attack, compare and contrast perimeter and layered approaches to network security
B2. Protect against various types of attacks
B3. Know how to protect a system
B4. Discuss modern cryptography methods, and select appropriate ones
B5. Evaluate the effectiveness of a scanner based on how it works
B6. Choose the appropriate type of firewall for a given organization
B7. Evaluate and improve network administration policies

C. Practical skills

C1. Acquire a working knowledge of several specific viruses
C2. Be familiar with some of the basic tools used by hackers
C3. Employ intrusion-detection systems to detect problems on a computer system
C4. Create policies for network administration
C5. Probe a system for vulnerabilities, and use vulnerability scanning tools

D. Transferable skills and personal qualities

D1. Prepare structured technical reports for lab work assignment
D2. Use the Internet to research articles on the subjects of this course; prepare a state-of-the art reports; deliver verbal communications.

Assessment of learning outcomes:

Learning outcomes A1-A5, B1-B7 are assessed by examinations; learning outcomes C1-C5 are assessed by lab works, seminars and workshops; learning outcomes D1 and D2 are assessed by seminars and/or workshops.

Assessment instruments:

Allocation of Marks	
Assessment Instruments	**Marks**
Midterm examination	**30%**
Final Exam (written unseen exam)	**40 %**
Assignments and research work	**30%**
Total	**100%**

** Make-up exams will be offered for valid reasons only with consent of the Dean. Make-up exams may be different from regular exams in content and format.*

Documentation and academic honesty:

- Handed reports must be presented according to the style specified in the assignment sheet
- Protection by copyright
- Avoiding plagiarism: Any stated plagiarism leads to an academic penalty

Course academic calendar

Week	**Basic and support material to be covered**	**Assignments/ Research work**
(1)	Introduction to computer and information security	
(2)	Networks	
(3)	Cyber stalking, fraud, and abuse	
(4)	Denial of Service Attacks	**Assignment 1**
(5)	Malware	
(6)	Techniques used by hackers	
(7)	Industrial espionage in cyberspace	**Assignment 2**

(8)	Encryption	
(9)	Security technology	
(10)	Security policies	
(11)	Network scanning and vulnerability scanning	
(12)	Cyber terrorism and information warfare	
(13)	Cyber detective	
(14)	Introduction to forensics	
(15)	Seminar	
(16)	**Final Exam**	

Expected workload: On average you need to spend 6 hours of study and preparation for each lecture.

Attendance policy: Absence from lectures and/or tutorials shall not exceed 15%. Students who exceed the 15% limit without a medical or emergency excuse acceptable to and approved by the Dean of the relevant college/faculty shall not be allowed to take the final examination and shall receive a mark of zero for the course. If the excuse is approved by the Dean, the student shall be considered to have withdrawn from the course.

Literature and supporting material:

1. Chuck Easttom: Computer Security Fundamentals, Third Edition, Pearson, 2016
2. William Stallings, Lawrie Brown: Computer Security, Principles and Practice, Third Edition, Pearson 2015
3. Mark Ciampa: Security+ Guide to Network Security Fundamentals, 6th Edition, Cengage learning, 2018
4. Theodor Richardson, Charles Thies: Secure Software Design, Jones & Barlett Learning, 2013

Reading Material:

Selected research papers