QFO-AP-VA-008	رمز النموذج :	اسم النموذج : خطة المادة الدراسية
2	رقم الإصدار: (Rev)	الجهة المصدرة: نائب الرئيس للشؤون الأكاديمية
2021-5-4	تاريخ الإصدار:	الجهة المدققة : اللجنة العليا لضمان الجودة
4	عدد صفحات النموذج :	

جامعة فيلادلفيا
Philadelphia University

Course Title: Information Security			**Course code: 0750446**	
Course Level: *4*			**Course prerequisite(s) and/or corequisite(s):** 0750340	
Lecture Time:			**Credit hours: 3**	
UR ☐	**FR** ☐	**DR** ☐	**C** ▮	**E** ☐

Academic Staff Specifics

Name	Rank	Office Number and Location	Office Hours	E-mail Address
Maram Bani Younes	**Assistance Professor**	**IT 331**		**mbaniyounes@philadelphia.edu.jo**

The Learning Style Used in Teaching the Course

The Learning Style			
Blended Learning ▮			
Electronic Learning ☐			
Face-to-Face Learning ☐			
Face-to-Face	**Electronic**	**Blended**	**Percentage**
	-	**%100**	

Course Description
This course is based on the textbook SECURITY+ GUIDE TO NETWOK SECURITY FUNDAMENTALS, Fourth Edition. It is not a course in cryptography. In addition to fundamentals, it takes an in-depth and comprehensive view of security by examining the attacks that are launched against networks and computer systems, the necessary defense mechanisms, and offers end-user practical tools and techniques to counter attacks. For a summary of the topics covered in each chapter, consult the textbook.

Course Objectives
It is imperative to comprehend the significance of information security in relation to our corporate operations.
Acknowledge the ramifications of data breaches.
Acquire knowledge pertaining to the methods and rationales underlying the classification of information.

It is advisable to exercise prudence when utilising the internet, electronic mail, and other forms of electronic communication.

Adhere to the established protocols of the Company with regards to network accessibility, utilisation of portable media and devices, as well as the implementation of physical security measures.

Understanding the appropriate procedures and timing for reporting confirmed or suspected instances of data breaches.

Course Components
Textbooks

1-Network security essentials : applications and standards, William Stallings, Harlow: Pearson Education Limited, 2014.

2- Information security and cyber laws, Sanjeev Puri

In addition to the above, the students will be provided with handouts by the lecturer.

Teaching methods:

Teaching Methods

Duration: 16 weeks, 48 hours in total Lectures: 33 hours, 2 per week (including 1-hour midterm exams) Tutorials: 15 hours, (1 hour per week) Report Presentation: 3 hours Homework: 3 assignments and one research report

.

Learning outcomes:

Learning Outcomes:

A. Knowledge and Understanding

A1. Define authentication services, List the account management procedures for securing passwords, Describe relevant cryptography algorithms and list the various ways in which cryptography is used, Define digital certificates, Describe the components of Public Key Infrastructure and describe the different transport encryption algorithms.

A2. Describe the challenges of securing information attacks, Identify the types of attackers, List various techniques for mitigating and deterring attacks.

B. Intellectual skills

B1. Analyse relevant features of Web application and compare them with those relevant to client-side attacks.

B2. Model and analyse various types of attacks.

C. Practical skills

C1. Apply relevant security principles to hosts, applications, and networks.

C2. Implement secure network administration principles.

D. Transferable Skills and Personal Qualities

D1. Prepare structured technical reports for assigned lab works.

Learning outcomes achievement:

A1, A2, B1, and B2 are achieved through lectures and assessed by quizzes and examinations.

C1 ,C2, and D1 are achieved and assessed by homework: practical and assignments

Assessment instruments

- Short reports and/ or presentations, and Short research projects
- Quizzes.
- Home works
- Final examination: 40 marks

Allocation of Marks	
Assessment Instruments	**Mark**
Mid Exam	**30**
Reports, research projects, Quizzes, Home works, Projects	**30**
Final examination:	**40**
Total	**100**

Documentation and academic honesty

- Documentation style (with illustrative examples)
- Protection by copyright
- Avoiding plagiarism.

Documentation and academic honesty

- Documentation style (with illustrative examples)
- Protection by copyright
- Avoiding plagiarism

- Practical works reports must be presented according to the style specified in the homework and practical work guide
- Any stated plagiarism leads to an academic penalty

The assignments that have work to be assessed will be given to the students in separate documents including the due date and appropriate reading material.

Documentation and Academic Honesty

Submit your homework covered with a sheet containing your name, number, course title and number, and type and number of the home work (e.g. assignment, and project).

Any completed homework must be handed in the class on the due date. After the deadline "zero" will be awarded. You must keep a duplicate copy of your work because it may be needed while the original is being marked.

You should hand in with your assignments:

- A brief report to explain your findings.
- Your solution of given problem

For the research report, you are required to write a report similar to a scientific research paper. It should include:

- *Ab-stract:* It describes the main synopsis of your paper.
- *Introduction:* It provides background information necessary to understand the research and getting readers interested in your subject. The introduction is where you put your problem definition, summary of contribution, related work, and is likely where the bulk of your sources will appear.
- *Methods (Algorithms and Implementation):* Describe your methods here. Summarize the algorithms (if any) generally, highlight features relevant to your project, and refer readers to your references for further details. Information from sources must be rephrased in own words, "copy-and-paste" from documents, found for example on the Internet, is NOT allowed. It is allowed to use short quotations, or figures, from other documents, but then the source MUST be clearly stated in the reference list (please check copy rights). Papers not fulfilling these rules will be failed.
- *Results and Discussion (Benchmarking and Analysis):* This section is the most important part of your paper. It is here that you demonstrate the work you have accomplished on this project and explain its significance. The quality of your analysis will impact your final grade more than any other component on the paper. You should therefore plan to spend the bulk of your project time not just gathering data, but determining what it ultimately means and deciding how best to showcase these findings.
- *Conclusion:* The conclusion should give your reader the points to "take home" from your paper. It should state clearly what your results demonstrate about the problem you were tackling in the paper. It should also generalize your findings, putting them into a useful context that can be built

upon. All generalizations should be supported by your data, however; the discussion should prove these points, so that when the reader gets to the conclusion, the statements are logical and seem self-evident.

- *Bibliography:* Refer to any reference that you used in your assignment. Citations in the body of the paper should refer to a bibliography at the end of the paper.

- **Protection by Copyright**

1. Coursework, laboratory exercises, reports, and essays submitted for assessment must be your own work, unless in the case of group projects a joint effort is expected and is indicated as such.
2. Use of quotations or data from the work of others is entirely acceptable, and is often very valuable provided that the source of the quotation or data is given. Failure to provide a source or put quotation marks around material that is taken from elsewhere gives the appearance that the comments are ostensibly your own. When quoting word-for-word from the work of another person quotation marks or indenting (setting the quotation in from the margin) must be used and the source of the quoted material must be acknowledged.
3. Sources of quotations used should be listed in full in a bibliography at the end of your piece of work.

- **Avoiding Plagiarism**

1. Unacknowledged direct copying from the work of another person, or the close paraphrasing of somebody else's work, is called plagiarism and is a serious offence, equated with cheating in examinations. This applies to copying both from other students' work and from published sources such as books, reports or journal articles.
2. Paraphrasing, when the original statement is still identifiable and has no acknowledgement, is plagiarism. A close paraphrase of another person's work must have an acknowledgement to the source. It is not acceptable for you to put together unacknowledged passages from the same or from different sources linking these together with a few words or sentences of your own and changing a few words from the original text: this is regarded as over-dependence on other sources, which is a form of plagiarism.
3. Direct quotations from an earlier piece of your own work, if not attributed, suggest that your work is original, when in fact it is not. The direct copying of one's own writings qualifies as plagiarism if the fact that the work has been or is to be presented elsewhere is not acknowledged.
4. Plagiarism is a serious offence and will always result in imposition of a penalty. In deciding upon the penalty the Department will take into account factors such as the year of study, the extent and proportion of the work that has been plagiarized, and the apparent intent of the student. The penalties that can be imposed range from a minimum of a zero mark for the work (without allowing resubmission) through caution to disciplinary measures (such as suspension or expulsion).

Course/Module Academic Calendar

Week	Basic and support material to be covered	Homework/reports and their due dates
(1)	Introduction to Security	
(2)	Malware and Social Engineering Attacks (1)	
(3)	Application and Network Attacks (1)	
(4)	Application and Network Attacks (2)	
(5)	Vulnerability Assessment and Mitigating Attack	
(6)	Host, Application , and Data Security (1)	
(7)	Host, Application , and Data Security (2) **Midterm exam**	
(8)	Network Security (1)	
(9)	Network Security (2)	
(10)	Administering a Secure Network	
(11)	Wireless Network Security	
(12)	Access Control Fundamentals	
(13)	Authentication and Account Management	
(14)	Basic Cryptography	

(15) **(Optional)**	Advanced Cryptography & project	
(16) **Final Examination**		

Expected workload
On average students need to spend 2 hours of study and preparation for each 50-minute lecture/tutorial.

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.

Module References
Students will be expected to give the same attention to these references as given to the Module textbook(s)

1. Mark Ciampa, Security+ Guide to Network Security Fundamentals, 4th Edition, Course Technology, 2012
2. William Stallings, Wireless Communications & Networks, 2nd edition, Prentice-Hall Pearson, 2005
3. Computer Networking: A top down approach 6th edition, J.F. Kurose and K.W. Ross,

Website(s):
http://ecourse.philadelphia.edu.jo/login/index.php // our e-course