Information Systems Department

Course Syllabus

IS380 – Cyber Security

Catalog Description: This course aims to provide students with an academic overview of cyber security covering its main domains. The course provides the foundation for understanding the key issues associated with protecting information using cryptographic algorithms, determining the authentication and authorization techniques for safe access to information, and assigning the features of information security protocols. In addition, the course will provide the student with an overview of the main software flaws and different ways of protections against intruders. Students will be exposed to the spectrum of security activities, methods, and techniques. By the completion of this course, students should appreciate the significance of information security in the IT realm, and be able to demonstrate in-depth knowledge of information security technical key principles and techniques. Upon successful completion of this course, students will have a broad ethical knowledge of the major technical security challenges.

Credit Hours: 3 Credit hours: 3 Lectures per week 0 Labs. per week 0 Recitation per week

Prerequisites: CS330- Computer Networks, IS321-Database Management Systems

Course Learning Outcomes:

1. Describe information security's importance in our increasingly computer-driven world.
2. Outline the key concepts of information security terminologies.
3. Describe the fundamental issues in designing access control models and authentication and security protocols.
4. List the main characteristics of software flaws and malicious software.
5. State information security ethics & laws.
6. Explain the main cryptography algorithms.
7. Plan and organize an information systems security development project at introductory level.
8. Function effectively on teams to accomplish a common goal.
9. Present a topic in a compelling manner.

Major Topics:

- Introduction to Cyber Security
- Basic Concepts of Threat, Evaluation of Assets, Information Assets, Physical, Operational, And Information Security
- Basic Cryptography and its Implementation
- Critical Security Principles, Creation and Maintenance of a Comprehensive Security Model
- Risk Assessment Frameworks, Risk Analysis and Risk Management
- Security Policy, Information Security Strategies

- Design of a Secure Organizational Information Infrastructure.
- Security Issues in Hardware, Software, Processes, Communications and Applications.
- Argue the place of ethics in the Information Security area.

- Project Discussions.

Text Books: Information Security Principles and Practice, 2nd edition, Mark Stamp, Wiley Publications, 2011, ISBN 978-0470626399.

Course Syllabus

IS380 – Cyber Security

Grading:

- The grading scale for this course is:

95 - 100	A+	Passing
90 - 94	A	Passing
85 - 89	B+	Passing
80 - 84	B	Passing
75 - 79	C+	Passing
70 - 74	C	Passing
65 - 69	D+	Passing
60 - 64	D	Passing
0 - 59	F	Failing

- Final grades will be determined based on the following components:
  . 60% Semester Work
  . 40% Final Exam
- Students may not do any additional work for extra credit nor resubmit any graded activity to raise a final grade.
- Late submissions will not be accepted for any graded activity for any reason.
- Students have one week to request the re-grading of any semester work.

Attendance Policy:

Students should attend 80% of the overall course hours taught in the semester as per the University regulations.

If a student fails to achieve this portion, he/she shall not be allowed to appear in the final exam and shall be awarded "DN" grade and repeat the course.

Cheating and Plagiarism Policy:

The instructor will use several manual and automated means to detect cheating and/or plagiarism in any work submitted by students for this course.

When a student is suspected of cheating or plagiarism, the instructor raises the issue to the disciplinary committee.

Course Syllabus

IS380 – Cyber Security

Communications:

Registered students will be given access to a section of the Learning Management System (LMS) for this course. LMS will used as the primary mechanism to disseminate course information, including announcements, lecture slides, assignments, and grades.

Communication with the instructor on issues relating to the individual student should be conducted using CIS email, via telephone, or in person.