Ministry of Higher Education and Scientific Research
Lebanese French University – Erbil
College of Engineering and Computer Science
Department of Information Technology

Information Security

Third Stage – First Semester

Asst. Prof. Dr. Saravana Balaji B

Academic Year: 2022-2023

Course Book

S. No.	Information	Details
1.	**Course Name**	Information Security
2.	**Course Code**	IT301IS
3.	**Lecturer In-charge**	Dr. Saravana Balaji B
4.	**College/Department**	College of Engineering & Computer Science / Department of Information Technology
5.	**Contact Information**	E-mail: saravanabalaji.b@lfu.edu.krd Mobile No.: 0964-7506740307
6.	**Time (in hours) per Week**	Theory:3
7.	**Office Hours**	8:30 AM-3:00PM
8.	**Teacher's Academic Profile**	**He has completed B.E, M.E and Ph.D in Computer Science and Engineering. He has Fifteen years of teaching experience in Computer Networks, Web Services, Cloud Computing and Semantic Web**
9.	**Academic Title**	Assistant Professor
10.	**Keywords**	▪ Information Security ▪ Cryptograph ▪ Attacks
11.	**Course Overview:** The Information Security course will provide the reader with a basic knowledge of information security in both theoretical and practical aspects. It will first cover the basic knowledge needed to understand the key concepts of information security, discussing many of the concepts that underpin the security world. It will then dive into practical applications of these ideas in the areas of operations, physical, network, operating system, and application security	
12.	**Aims & Objective:** Learning Objectives includes Upon completing this course, students will: - Understand the fundamentals of Information security - Understand the legal aspects of security for digital data - Understanding the Tools that used for this courses and how to used it (some tools for file system and E-mail) - Understand the relationship between IT and security - Learn best practices for incidence response	
13.	**Course Requirement:** Attendance and completion of all tests, exams, reports.	
14.	**Teaching and Learning Method:** ▪ Book, Data Show and PowerPoint, white board, Lectures, homework's, and assignments.	

15.	**Assessment Scheme:** ▪ 25 % Mid-term Examination ▪ 15 % Assignments and Quizzes ▪ 60 % Final Examination
16.	**Students Learning Outcome:** At the end of this course the student will be able to: 1. Develop an understanding of information assurance as practiced in computer operating systems, distributed systems, networks and representative applications. 2. Gain familiarity with prevalent network and distributed system attacks, defenses against them, and forensics to investigate the aftermath. 3. Develop a basic understanding of cryptography, how it has evolved, and some key encryption techniques used today. 4. Develop an understanding of security policies (such as authentication, integrity and confidentiality), as well as protocols to implement such policies in the form of message exchanges. 5. Determine appropriate mechanisms for protecting information systems ranging from operating systems to database management systems and to applications.
17.	**Course Reading List and References** **Textbooks** 1. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, 1st Edition Jason Andress, Syngress Publications 2. William Stallings, "Cryptography and Network Security", Fourth edition, PHI ○ Schneier, Bruce, "Applied Cryptography", John Wiley and Sons
18.	**Course Content**

Course Content

Week	Lecture Date	No. of Hours	Topics
1.	Week 1	4	Introduction to Information Security – Models for Security Issues
2.	Week 2	4	Defenses – Type of Attacks, controls
3.	Week 3	4	Identification & Authentication
4.	Week 4	4	Authorization & Access Controls
5.	Week 5	4	Access Control Models
6.	Week 6	4	Auditing & Accountability

7.	Week 7	4	Cryptography – Introduction
8.	Week 8	4	Modern Cryptographic tools & methods
9.	Week 9	4	Operations Security & Physical Security controls
10.	Week 10	4	Network Security – Firewalls, Network Intrusion Detection
11.	Week 11	4	Network Security – VPN, Wireless network security, secure protocols
12.	Week 12	4	Network Security Tools – Scanners, packet sniffers, honeypots
13.	Week 13	4	Operating Systems Security – OS Hardening
14.	Week 14	4	OS security – Malwares, firewalls, host intrusion detection
15.	Week 15	Examination	

19.	**Examinations:** 1. Explain in detail about models for information security 2. Explain about various cryptographic methods 3. Illustrate the significance of firewall in network security 4. Justify why operating systems security is important and its tools 5. Explain about tools and techniques of web security in detail.
20.	**Course Policy:** Designed to educate students about information security policies, standards, and procedures along with risks to information and information systems.
21.	**Note:** Students will work in groups to prepare a 20-minute presentation on a topic of their choosing. The presentations will be conducted during the last few weeks of class