Course Title:	**IT Security**
Course Code:	CSE531/1
Program:	Master Degree In Computer Engineering
Department:	Computer Engineering
Course coordinator:	Amina GHARSALLAH
Institution:	Private Higher School of Engineers of Gafsa (ESIP)

A. Course Identification

1. Credit hours: **3 (1.5-1.5-0)**

2. Course type

a. College ☐ Department ■ Others ☐

b. Fundamental ■ Transversal ☐ Optional ☐

3. Level/year at which this course is offered: 3.1/3

4. Pre-requisites for this course (if any): Networking Fundamentals, Operating Systems: Foundational Knowledge of Computer Science

5. Co-requisites for this course (if any)**:**

1. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours	Self-study	Total workload
1	**Traditional classroom**	…..	22	52
2	**Blended**	30		
3	**E-learning**	.....		
4	**Distance learning**	.....		
5	**Other ()**	.....		

2. Contact Hours (based on academic semester)

No	Activity	Contact Hours
1	**Lecture**	15
2	**Laboratory/Studio**	15
3	**Tutorial**	-
4	**Others** (specify)	-
	Total	30

B. Course Objectives and Learning Outcomes

Course Description

The course aims to provide engineering students with a solid foundation in the principles and concepts of IT security. It covers the basic terminology, components, and technologies used in securing computer systems, networks, and data. The course focuses on increasing students' awareness of various security threats and vulnerabilities in the IT domain. It helps them understand the potential risks associated with cyber attacks, malware, social engineering, and other common security breaches.

Course Main Objective

At the end of the module, the student should be able to:
Develop an in-depth knowledge on fundamental IT security concepts and principles.
Develop skills in recognizing and assessing common security threats and vulnerabilities faced by computer systems, networks, and information resources, such as malware, social engineering attacks, data breaches, and network intrusions.
Inderstand different types of security controls: and Develop practical skills in securing systems and networks.

1. Course Learning Outcomes

CLOs		Aligned PLOs
1	**Knowledge and Understanding**	
1.1	✓ Understand the fundamental concepts of IT security, including confidentiality, integrity, and availability.	PLO.K1
2.1	✓ Apply secure coding practices to develop and maintain secure web applications	PLO.K2
2.2	✓ Analyze data protection techniques, including encryption, access controls, and data masking.	PLO.K3
2	**Skills**	
2.1	✓ Develop critical thinking skills to analyze security issues and make informed decisions	PLO.S2
3.1	✓ Conduct risk assessments and create risk management plans.	PLO.S3
4.1	✓ Develop a deeper understanding and appreciation of cultural diversity through their participation in cultural events and international computer security clubs.	PLO.S4
6.1	✓ Monitor network traffic for security incidents and respond to threats effectively.	PLO.S6
7.1	✓ Implement security features in web development, including authentication and authorization.	PLO.S7

C. Course Content

No	List of Topics	Contact Hours
1	Chapter 1: Introduction to IT Security • Overview of IT security fundamentals • Importance of IT security in today's digital landscape • Key principles and concepts in IT security	3
2	Chapter 2: Risk Assessment and Management • Conducting risk assessments and threat modeling • Identifying vulnerabilities and potential impacts • Developing risk mitigation strategies and incident response plans	3
3	Chapter 3: Cryptography and Data Protection • Fundamentals of cryptography • Symmetric and asymmetric encryption algorithms • Securing data at rest and in transit	3
4	Chapter 4: Network Security • Network infrastructure security • Firewalls, IDS/IPS, and network monitoring • Securing wireless networks	3
5	Chapter 5: Security in Web Applications • Common vulnerabilities in web applications • Best practices for secure coding • Web application firewalls and secure development frameworks	3
6	Labs: • Lab 1 : Detection of threats and vulnerabilities (Nmap/nessus/ettercap) • Lab 2 : Using the OpenSSL cryptographic toolbox • Lab 3 : Traffic Filtering on Cisco Packet Tracer • Lab 4 : Deploying Snort and exploring Cisco IOS IPS • Lab 5 : Creating a VPN Tunnel on Cisco Packet Tracer	15
Total		30

D. Teaching and Assessment

1. Alignment of Course Learning Outcomes with Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
1.0	**Knowledge and Understanding**		
PLO.K1	✓ Understand the fundamental concepts of IT security, including confidentiality, integrity, and availability.	• Lectures • Hands-On Labs • Group Discussions • Research Projects	• Exam, Quizzes, Homework assignments Practical Work
PLO.K2	✓ Apply secure coding practices to develop and maintain secure web applications		
PLO.K3	✓ Analyze data protection techniques, including encryption, access controls, and data masking.		
3.0	**skills**		
PLO.S2	✓ Develop critical thinking skills to analyze security issues and make informed decisions	✓ Lectures ✓ Hands-On Labs ✓ Group Discussions Research Projects	▪ Exam, Quizzes, Homework assignments ▪ Practical Work
PLO.S3	✓ Conduct risk assessments and create risk management plans.		
PLO.S4	✓ Develop a deeper understanding and appreciation of cultural diversity through their participation in cultural events and international computer security clubs.		
PLO.S6	✓ Monitor network traffic for security incidents and respond to threats effectively.		
PLO.S7	✓ Implement security features in web development, including authentication and authorization.		

2. Assessment Tasks for Students

	Assessment task*	Week Due	Percentage of Total Assessment Score
1	Practical Work (written or oral)	Weekly	00 %
2	Quizzes, Homework assignments	Random	00 %
3	First mid Term	-	00 %
4	Final Exam	11	100 %

E. Student Academic Counselling and Support

Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice:
1- Office hours 2- Blackboard interface

F. Learning Resources and Facilities

1. Learning Resources

Required Textbooks	1. Wendell Odom, CCNA 200-301 Official Cert Guide, Volume 1, 2019 2. Wendell Odom, CCNA 200-301 Official Cert Guide, Volume 2, 2019 3. Stallings, W. (2017). "Cryptography and Network Security: Principles and Practice." Pearson. 4. Schneier, B. (2015). "Secrets and Lies: Digital Security in a Networked World." Wiley. 5. Anderson, R. (2020). "Security Engineering: A Guide to Building Dependable Distributed Systems." Wiley. 6. Whitman, M. E., & Mattord, H. J. (2017). "Management of Information Security." Cengage Learning.
Essential References Materials	NA
Electronic Materials	1. Cisco Cybersecurity Training & Certifications (cisco.com) 2. Cybersecurity & Ethical Hacking Courses – Coursera, Udemy, Cybrary
Other Learning Materials	NA

2. Facilities Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	**classroom board software …**
Technology Resources (AV, data show, Smart Board, software, etc.)	**data show;**

G. Course Quality Evaluation

EvaluationAreas/Issues	Evaluators	Evaluation Methods
Effectiveness of teaching and assessment.	Students, Faculty, Program Leaders, Peer Reviewer	Direct/Indirect
Extent of achievement of course learning outcomes.	Faculty, Program Leaders, Peer Reviewer	Direct, Indirect
Quality of Learning resources	Faculty, Program Leaders, Peer Reviewer	Direct, Indirect
Teaching and learning quality and effectiveness.	Students, Faculty Program Leaders, Peer Reviewer	Direct, Indirect

H. Specification Approval Data

Council / Committee	Computer Engineering Council
Date	11/09/2023