

ITEC-331 Fundamentals of IT

General Information

Course Code	ITEC 331	Level/Year	5 /2025	Required (R)/ Selected Elective (SE)			R
Credit Hours	Theory		2	Lab	1	Total	3
Prerequisites	ITEC-331						
Course Coordinator	SABNA MACHINCHERY ALI						

Course Description

This introductory course will provide learners with principles of data and technology that frame and define cyber security. Students will gain insight into the importance of cyber security and the integral role of cyber security professionals. This course will provide a dynamic learning experience for the students with foundational cyber security principles, security architecture, risk management, attacks, incidents, and emerging IT security technologies.

Topics may include confidentiality, integrity, and availability; security architecture; security policies; authentication; access control; risk management; threat and vulnerability assessment; common attack/defense methods; IDPS ;incidence response plan; introduction to cryptography.

Course Objectives

- ◆ Define Key concept of Security
- ◆ Explain the core information security principles
- ◆ Identify the key components of cyber security network architecture
- ◆ Describe risk management processes and practices
- ◆ Distinguish system and application security threats and vulnerabilities
- ◆ Appraise cyber security incidents to apply appropriate response
- ◆ Evaluate decision making outcomes of cyber security scenarios
- ◆ Develop and apply skill in information security using Kali Linux

Course Contents

List of Topics	Weeks
UNIT 1: What is Security.	1,2
UNIT 2: The Need For Security & Cyber security Architecture	3, 4, 5
UNIT 3: Risk Management Process & Practices	5, 6, 7
UNIT 4: Security Technology	8, 9, 10
UNIT 5: Cyber security Incidents To Apply Appropriate Response	10, 11, 12
UNIT 6: Cryptography	13, 14, 15

Textbook

Principles of Information Security, 6th Edition, Michael E. Whitman, Herbert J. Mattord, 2018, Cengage, Print ISBN: 9781337102063.

Reference Materials

Information Security: Principles and Practices, 2nd Edition, Mark S. Merkow, Jim Breithaupt, 2014, Publisher Pearson Education ISBN-13: 978-0-7897-5325-0.

Foundation of information security by Jason Andress. ISBN-10: 1-7185-0004-1, ISBN-13: 978-1-7185-0004-4, Publisher: William Pollock




Course Learning Outcomes

CLO	Description	Level of Learning (LOL)	Mapped PI
CLO#01	Understand the key concept, critical characteristics and components of information security, Different software attacks, risk management, incidence response plan, IDPS and basic concept of Cryptography.	Knowledge	PI 1.1
CLO#02	Define Security, Attack, vulnerability, Cyber security architectures, .risk management, Data breach, incidence response and cryptanalysis.	Comprehension	PI 1.2
CLO#03	Identify different attacks, risk control method, Types of IDPS, incidence response plan and encryption method.	Comprehension	PI 1.3
CLO#04	Recognize Approaches to Information Security Implementation ,Why business need IT, Various activities of identifying, assessing and controlling the risk management processes and practices ,Why use IDPS ,IDPS strength and Limitation and Encryption methods. Hash function and message authentication	Applying	PI 2.2
CLO#05	Implement CIA triad in real life situations, select an IDPS response behaviour, Implement how to prevent same incident in future and apply different cryptographic method,	Applying	PI 2.3
CLO#06	Write clear and concise technical documentation of recent security breaches and their solutions for various audience.. Deliver oral presentation on mini project	Comprehension	PI 3.1 PI 3.2

CLO-SO-PI Mapping

CLOs	SOs					
	SO1	SO2	SO3	SO4	SO5	SO6
CLO#01	PI 1.1	-	-	-	-	-
CLO#02	PI 1.2	-	-	-	-	-
CLO#03	PI 1.3	-	-	-	-	-
CLO#04	-	PI 2.2	-	-	-	-
CLO#05	-	PI 2.3	-	-	-	-
CLO#06	-	-	PI 3.1 PI 3.2	-	-	-

Approvals

Prepared by Course Coordinator	SABNA MACHINCHERY ALI		
Approved by Track Leader	SABNA MACHINCHERY ALI	TL Signature	
Last updated	August 18, 2024		

