Course Name: FUNDAMENTALS OF IT SECURITY Course Code: ITEC 331

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	**NIL**	**Course Coordinator**		**SABNA MACHINCHERY ALI**		
Corequisites	**NIL**	**Track Leader**		**Dr. RAHAMA SALMAN**		

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 : On completion of the course, the student will be able to:

- 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
CH 1: What is Security.	1,2
CH 2: The Need For Security & Cyber security Architecture	3, 4, 5
CH 3: Risk Management Process & Practices	5, 6, 7
CH 4: Security Technology	8, 9, 10
CH 5: Cyber security Incidents To Apply Appropriate Response	10, 11, 12
CH 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	Mapped PI
CLO#01	**Understand** the key concept of information security and cryptography.	PI 1.1
CLO#02	**Define** terminologies of information security and cryptography.	PI 1.2
CLO#03	**Identify** different attacks, risk control method and IDPS.	PI 1.3
CLO#04	**Recognize** the different approaches to information security implementation and incidence response plan. Manage secure computing environment by identifying and mitigating threats and vulnerabilities.	PI 2.2 PI 6.4
CLO#05	**Implement** information security knowledge and skills in real life scenarios. Develop and apply computing solutions for security requirements using Kali Linux.	PI 2.3 PI 6.1
CLO#06	**Write** clear and concise technical documentation of recent security breaches and their solutions for various audience.. Deliver oral presentation on mini project	PI 3.1 PI 3.2

CLO-PI-SO Mapping

	SO-1	SO-2	SO-3	SO-4	SO-5	SO-6
CLO#01	PI 1.1	-	-	-	-	-
CLO#02	PI 1.2	-	-	-	-	-
CLO#03	PI 1.3	-	-	-	-	-
CLO#04	-	PI 2.2	-	-	-	PI 6.4
CLO#05	-	PI 2.3	-	-	-	PI 6.1
CLO#06	-		PI 3.1 PI 3.2	-	-	