d)	Seminar	5
e)	Book/ Article Review	
f)	Viva-Voce	
g)	Field Report	
Grand Total		**75**

KU4VACCSC107: INFORMATION SECURITY

Semester	Course Type	Course Level	Course Code	Credits	Total Hours
4	VAC	100-199	KU4VACCSC107	3	45

Learning Approach (Hours/ Week)			Marks Distribution			Duration of ESE (Hours)
Lecture	Practical/ Internship	Tutorial	CE	ESE	Total	
3	0	-	25	50	75	1.5 hrs.

Course Description:

This course introduces the basics of information security, covering key concepts such as the importance of security policies, the CIA Triad, threats and vulnerabilities, and common security measures. Students will learn about cryptography, including symmetric and asymmetric key systems, and explore network security fundamentals and ethical considerations in information security. The course aims to provide a foundational understanding of information security principles and practices.

Course Prerequisite: NIL

Course Outcomes:

CO No.	Expected Outcome	Learning Domains

1	Identify the foundational concepts and principles of information security.	U
2	Understand the principles of confidentiality, integrity, and availability in information security.	U
3	Recognize different types of security threats and vulnerabilities.	U
4	Understand cryptographic techniques in securing data	U
5	Identify network security protocols and technologies to secure network communications.	U

* ***Remember (R), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C)***

Mapping of Course Outcomes to PSOs

	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	PSO 6	PSO 7
CO 1	3			3			
CO 2	3			3			3
CO 3	3			3			3
CO 4	3	2	2				
CO 5	3			3			3

COURSE CONTENTS

Contents for Classroom Transaction:

MODULE	UNIT	DESCRIPTION	HOURS
1	**FOUNDATIONS OF INFORMATION SECURITY**		

	1	**Foundations of Information Security**	9
		a) Definition, Importance of Information Security	
		b) Evolution of Information Security	
	2	**Security Policies, Standards, and Guidelines**	
		a) Overview of Security Policies, Types of Security Standards	
	3	**CIA Triad**	
		a) Confidentiality, Integrity, Availability	
		b) Balancing the CIA Triad: Trade-offs and Challenges	
	4	**Threats and Vulnerabilities**	
		a) Types of Threats	
		b) Attacks and Malwares	
		c) Firewalls, Common Security Vulnerabilities	

2	**CRYPTOGRAPHY**		
	1	Cryptography Techniques: Basic Terms, Plain Text, Cipher text, Substitution Techniques, Transposition Techniques, Fiestel Cipher.	9
	2	Encryption, Decryption, Symmetric and asymmetric key Cryptography. Symmetric Key Encipherment - Traditional symmetric Key Ciphers: Introduction-Kirchhoff's principle, cryptanalysis.	
	3	Categories of traditional ciphers; Substitution Ciphers- mono-alphabetic ciphers, polyalphabetic ciphers	
	4	Transposition Ciphers-keyless and keyed transposition ciphers, Stream and Block Ciphers-steganography.	

3	**Public key cryptography**		
	1	Public key Cryptosystem: Principles of Public Key Cryptosystems; Applications of public Key Crypto systems.	9
	2	Requirement for Public Key Cryptosystem, Public Key Cryptanalysis. RSA Algorithm–Description of the Algorithm, The security of RSA	
		3.Digital Signature:-Comparison between conventional and digital signature-Inclusion,Verification, Relationship, Duplicity; Process-needs for keys, signing the digest; scheme.	

		4.Services-message authentication, message integrity, non-repudiation, confidentiality. Digital signature Forgery and types- Digital Signature Schemes-RSA digital signature scheme.	

4	**Authentication Mechanisms**		
	1	Authentication Basics, Passwords, Biometric Authentication	9
	2	Key Distribution Center, Security handshake Pitfalls, Attacks on Authentication Schemes.	
	3	Firewalls: Architecture, Generation and Types. Virtual Private Network.	
		4.Email Security: PGP and S/MIME.	

5	**Teacher Specific Module**	
	Directions	
	1. Encryption and Decryption with Caesar Cipher 2. Symmetric Key Encryption using DES 3. Public Key Encryption with RSA 4. Digital Signature Generation and Verification	9

Essential Readings:

1. Behrouz A. Forouzan and Debdeep Mukhopadhyay, Cryptography And Network Security, 3rd Ed, McGraw Hill (Units I, II, IV)
2. William Stallings, Cryptography and Network Security - Principles and Practice Paperback, 7th Ed, Pearson (Unit III)
3. Dr. Wm. Arthur Conklin, Dr. Gregory White, "Principles of Computer Security Sixth Edition", McGraw Hill.

Suggested Readings:

5. Tavani, H. T. Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing. Wiley.

Assessment Rubrics:

Evaluation Type	Marks

End Semester Evaluation		**50**
Continuous Evaluation		**25**
a)	Test Paper- 1	5
b)	Model Examination	10
c)	Assignment- 2 Numbers	5
d)	Seminar/viva	5
e)	Book/Article review	
f)	Field report	
Grand Total		**75**