C. U. SHAH UNIVERSITY
Wadhwan City

FACULTY OF: - Technology and Engineering
DEPARTMENT OF: - Information Technology
SEMESTER: - VII
CODE: - **4TE07ISE1**
NAME: – **Information Security**

Teaching & Evaluation Scheme: -

Subject Code	Subject Name	Teaching Scheme (Hours)				Credits	Evaluation Scheme							
							Theory				Practical (Marks)			Total
							Sessional Exam		University Exam		Internal		University	
		Th	Tu	Pr	Total		Marks	Hours	Marks	Hours	Pr/Viva	TW	Pr	
4TE07ISE1	Information Security	3	0	2	5	4	30	1.5	70	3	-	20	30	150

Objectives:
The learning objectives of this course are to:

- To understand the major concepts of Information Security, Cyber Security and Forensics and to create the awareness through simple practical tips and tricks and to educate the students to learn how to avoid becoming victims of cyber crimes.
- The subject and the course content will help to the student who wish to take up cyber forensics as career as well as those who want to seek careers in cyber security.
- To gain experience of doing independent study and research in the field of cyber security and cyber forensics.

Prerequisites:

- Basic fundamental knowledge of Cryptography & Network Security and Programming Language.

Course outline:

Sr. No.	Course Contents	Total Hrs.
1	**Introduction:** Information Security, Cyber Security, Cyber Crime, Hacker, Cracker, Information Security Basics Public and Private Key Infrastructure, Network and Security Concepts Information Assurance Fundamentals : Authentication, Authorization , No repudiation ,Confidentiality, Integrity ,Availability.	08
2	**Exploits:** Viruses and it's types , Worms, Malware, Botnets Techniques to Gain a Foothold: Shell code ,Integer Overflow Vulnerabilities, Stack-Based Buffer Overflows ,Stacks upon Stacks Protecting against Stack-Based Buffer Overflows, SQL Injection and protection against it, Phishing, DoS Attacks , Backdoor Exploits , Server Exploits, O.S Exploits.	10
3	**Web Threats:** Client: Spoofing, Repudiation, Tampering with data, Phising, Password Sniffing, Identity Theft; Server: Eavesdropping, Unauthorized	10

	Access, Access Control, DoS, Network Hijacking; Service: Unauthorized access, Reconnaissance, Bypassing of firewalls, DDoS.	
4	**Digital Forensic:** Digital Forensics , Life Cycle ,Chain of Custody Concepts, Approaching a Investigation, Network Forensics ,Computer Forensics, Challenge, Forensic Auditing, Analysis Tools: Authorship Analysis.	**08**
5	**Cyber Laws:** Need for Cyber Law, Legal Landscape Around the World, Indian IT Act 2000, IT Act 2008 and its Challenges, Cybercrime Punishments.	**04**
6	**Firewalls and Intrusion Detection Systems:** Firewalls: Working, Types, Challenges. IDS: Introduction, Prevention Versus Detection, types of IDS.	**05**
	Total	**45**

Learning Outcomes:

- To gain concepts of Web Threats and Vulnerability.
- To gain concepts of Cyber Law and Digital Forensic.

Books Recommended:

1. "Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives" by Nina Godbole, Sunit Belapur, Wiley India Publications
2. "Network Security and Cryptography" by Bernard Menzes, Cengage Learning
3. "Cyber Security Essentials" by James Graham, Richard Howard, Ryan Olson, Auerbach Publication
4. "Software Forensics" by Robert M. Slade, Tata McGraw-Hill Publication
5. "Cryptography and Network Principles and Practice" by William Stallings, Pearson Publication.