BCSE317L	INFORMATION SECURITY	L	T	P	C
		3	0	0	3
Pre-requisite		**Syllabus version**			
		1.0			

Course Objectives

1. To learn various threats and attacks in a network.
2. To understand and explore fundamental techniques in developing secure applications.
3. To learn various methodologies for securing information systems ranging from operating systems to database management systems and to applications.

Course Outcomes

After completion of this course, the student shall be able to:

1. Apply fundamental knowledge on key security concepts, access control and authentication.
2. Comprehend the use of security techniques for securing the information.
3. Apply various data privacy policies in different areas of web based security systems.
4. Differentiate the needs and application of security in Operating System and Firewalls.
5. Analyze various method of securing databases.

Module:1	**Information Security Concepts**	**4 hours**

Information Security - Computer Security - Threats - Harm - Vulnerabilities - Program Security - Malicious code - Malwares: Viruses, Trojan Horses and Worms - Counter measures.

Module:2	**Authentication and Access Control**	**6 hours**

Authentication - Key management schemes - Hierarchical Key Management Techniques - Security Standards - User Authentication Protocols - Implementing Access Controls - Access Control Models - Role Based Access Control - Attribute Based Access Control - Attribute based Encryption in Information Storage - Physical Access Controls.

Module:3	**Operating Systems Security**	**7 hours**

Security in Operating System - Security in the design of OS: Simplified Design, Layered Design, Kernelized design, Reference Monitor, Trusted Systems, Trusted Systems Functions - Trusted Operating System Design - Rootkit.

Module:4	**Security Countermeasures**	**7 hours**

Design of Firewalls - Types - Personal Firewalls - Configurations - Network Address Translation - Data Loss Prevention - Intrusion Detection and Prevention Systems: Types of IDSs, Intrusion Prevention system, Intrusion Response, Goals of IDSs, Strength and Limitations.

Module:5	**Database Security**	**6 hours**

Database Security - Database Security Requirements - Reliability and Integrity - Sensitive Data - Types of Disclosures - Preventing Disclosures - Inference - Multilevel Databases - Multilevel Security - Database Attacks - SQL Injection Attacks.

Module:6	**Web Security**	**6 hours**

Browser Attacks: Types, Failed Identification and Authentication - Misleading and Malicious Web Contents - Protection against Malicious Web Pages - Website Data: Code within Data, Cross Site Scripting Attacks - Prevention of Data Attacks - Fake e-mails - Spam Detection - Phishing Attacks - Phishing URL Detection and Prevention.

Module:7	**Privacy Issues**	**7 hours**

Privacy Concepts: Aspects of Information Privacy, Computer-Related Privacy Problems - Threats to Personal Data Privacy - People-Based Privacy Concerns - Privacy Principles and Policies - Individual Actions to Protect Privacy - Governments and Privacy - Identify Theft - Privacy issues on the Web Data - Application of Cryptographic Techniques for Privacy Preservation.

Module:8	**Contemporary Issues**	**2 hours**
	Total Lecture hours:	**45 hours**

Text Book			
1.	Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, Security in Computing, 2018, Fifth Edition, Pearson, New York.		
Reference Books			
1.	Mark Stamp, Information Security: Principles and Practice, 2021, 3rd Edition, Wiley.		
2.	Joanna Lyn Grama, Legal and Privacy Issues in Information Security, 2020, 3rd Edition, Jones and Bartlett Publishers, Inc.		
Mode of Evaluation: CAT / written assignment / Quiz / FAT			
Recommended by Board of Studies	04-03-2022		
Approved by Academic Council	No.65	Date	17-03-2022