Course Code	Course Name	Course Type	Cd	L	T	P	Marks		
							Sessional	Final Exam	Total
COM-303	Foundations of Cyber Security	PCC	3	3	0	0	50	100	150

Course Outcomes:

At the end of the course, the student will be able to	
CO1	Explain cyber security principles to secure network and information systems.
CO2	Analyze cyber-attack techniques to improve defensive strategies.
CO3	Evaluate exploitation techniques to prevent and mitigate vulnerabilities.
CO4	Design strategies to defend against advanced persistent threats and malicious code.
CO5	Create incident response plans and perform forensic analysis to handle security breaches.

Detailed Syllabus

Section-A

Unit 1: Cybersecurity Introduction- Computer Security, Threats, Harm, Vulnerabilities, Controls, Authentication, Access Control, Cryptography: Problems Addressed by Encryption, Terminology, DES: The Data Encryption Standard, AES: Advanced Encryption System, Public Key Cryptography, Digital Signatures. **(8 Hrs.)**

Unit 2: Programs and Programming: Unintentional (Non-malicious) Programming Oversights, Malicious Code—Malware, Countermeasures. **Web Security:** User Side, Browser Attacks, Web Attacks Targeting Users, Obtaining User or Website Data, Email Attacks. **Operating Systems Security:** Security in Operating Systems, Security in the Design of Operating Systems, Rootkit. **(10 Hrs.)**

Unit 3: Network Security: Network Concepts, Threats to Network Communications, Wireless Network, Security, Denial of Service, Distributed Denial-of-Service. **Strategic Defenses:** Security, Countermeasures, Cryptography in Network Security, Firewalls, Intrusion Detection and Prevention Systems, Network Management. **(8 Hrs.)**

Unit 4: Cloud Computing and Security: Cloud Computing Concepts, Moving to the Cloud, Cloud, Security Tools and Techniques, Cloud Identity Management, Securing IaaS. **Privacy:** Privacy Concepts, Privacy Principles and Policies, Authentication and Privacy, Data Mining, Privacy on the Web, Email Security, Privacy Impacts of Emerging Technologies. **(10 Hrs.)**

Unit 5: Management and Incidents: Security Planning, Business Continuity Planning, Handling Incidents, Risk Analysis, Dealing with Disaster. **Legal Issues and Ethics:** Protecting Programs and Data, Information and the Law, Rights of Employees and Employers, Redress for Software Failures, Computer Crime, Ethical Issues in Computer Security, Incident Analysis with Ethics. **(8 Hrs.)**

Text Books

S. No.	Name of the Books	Author	Publisher	Edition (Pub. Yr.)
1	Security in Computing	Charles P. Pfleeger, Shari Lawrence Pfleeger, and Jonathan Margulies	Prentice Hall	5th (2018)

Reference Books

S. No.	Name of the Books	Author	Publisher	Edition (Pub. Yr.)
1	Information Security: The Complete Reference	Salvatore J. Stolfo, Steven M. Bellovin, Shlomo Hershkop, Angelos D. Keromytis	McGraw Hill	3rd (2017)
2	Information Security Management Handbook	Harold F. Tipton, CISSP . Micki Krause, CISSP	CRC Press	6th (2007)