CSOE-005: Cyber Security

Course Objectives:

- Exhibit knowledge to secure corrupted systems, protect personal data, and secure computernetworks in an Organization.
- Practice with an expertise in academics to design and implement security solutions.
- Understand key terms and concepts in Cryptography, Governance and Compliance.
- Develop cyber security strategies and policies
- Understand principles of web security and to guarantee a secure network by monitoringand analyzing the nature of attacks through cyber/computer forensics software/tools.

Credits: 03 **L-T-P-J: 3-1-0-0**

Unit-1: **8 Hours**

Introduction: Security threats, Sources of security threas- Motives - Target Assets andvulnerabilities – Consequences of threats- E-mail threats - Web-threats - Intruders andHackers, Insider threats, Cyber crimes. Network Threats: Active/ Passive – Interference –Interception –Impersonation – Worms –Virus – Spam's – Ad ware - Spy ware – Trojans andcovert channels –Backdoors – Bots – IP, Spoofing - ARP spoofing - Session Hijacking -Sabotage-Internal treats Environmental threats - Threats to Server security.

Unit-2: **8 Hours**

Security Threat Management: Risk Assessment - Forensic Analysis - Security threat correlation – Threat awareness - Vulnerability sources and assessment- Vulnerability assessment tools –Threat identification - Threat Analysis - Threat Modeling - Model for Information Security Planning.

Unit-3: **8 Hours**

Security Elements: Authorization and Authentication - types, policies and techniques – Securitycertification - Security monitoring and Auditing - Security RequirementsSpecifications – Security Policies and Procedures, Firewalls, IDS, Log Files, Honey Pots

Unit-4: **8 Hours**

Trusted Computing and multilevel security:- Security models, TrustedSystems, Software security issues, Physical and infrastructure security, Human factors –Security awareness, training , Email and Internet use policies.

Unit-5: **8 Hours**

DIGITAL FORENSICS: Introduction to Digital Forensics - Forensic Software and Hardware - Analysis and Advanced Tools -Forensic Technology and Practices - Forensic Ballistics and Photography - Face, Iris and FingerprintRecognition - Audio Video Analysis - Windows System Forensics - Linux System Forensics -Network Forensics.

Referential Books:

- Swiderski, Frank and Syndex, "Threat Modeling", Microsoft Press, 2004.
- William Stallings and Lawrie Brown, "Computer Security: Principles and Practice",Prentice Hall, 2008.

- Joseph M Kizza, “Computer Network Security”, Springer Verlag, 2005
- Thomas Calabres and Tom Calabrese, “Information Security Intelligence: CryptographicPrinciples & Application”, Thomson Delmar Learning, 2004.

Course Outcome:

- Understand the various ideas about cybercrime.
- Describe the Cyber Crime Strategy.
- Identify the Cyber Crime Investigation Methodology.
- Generalize the knowledge on Digital Forensics.
- ApplytheConceptsofCyberCrimeandDigitalForensicsinRealTimeScenarios.