Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME II Year Information Technology (Sp. Information Security) Semester- B			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ISR2C2: Digital Forensics and Security Audit	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Duration of Theory Paper: 3 Hours	**3**	**1**	**2**	**3**	**1**	**1**	**5**

Course Objective:

At the completing of the course, students will be able to understand the fundamental concepts of forensic science and digital forensics principles. Learn to identify importance of digital evidence.

COURSE CONTENT

Unit I : Introduction of Digital Forensics:

Digital crime, current scenario of digital crime in India, Evidence and its role in IT Act, Digital Evidence, Digital Vs Physical Evidence, nature of Digital Evidence, precautions while dealing with Digital Evidence, challenging aspects of Digital Evidence, Digital Devices, evidential potential of digital devices, Digital Forensics, dimensions and principles of Digital Forensics, Digital Forensic Investigation, Investigation Models, Scientific method in Digital Investigation, Research potential and scope in digital forensics.

Unit II : Data and Evidence Recovery:

Seizure of digital information : Issues, methodology, factors limiting wholesale seizure, pulling the plug or not; data objects, Storage Media, Variety of data, Recovered data objects, electronic evidence: secure boot and write blockers, disk file organization ,disk and file imaging; forensic tools, forensic data carving, data recovering techniques.

Unit III : Mobile and Live Forensics Investigations:

Mobile phone forensics: mobile device characteristics, memory considerations, tools classification, flasher boxes, obstructed devices, forensics procedures: preservation, acquisition, examination and analysis, reporting; SIM Card Forensics.

Network Forensics: sources of network based evidences, procedure for applying network based forensics, digital evidence on internet, digital evidence on physical and data link layers, digital evidence at the network and transport layers.

Unit IV : Security Issues and Principles:

Risk Analysis: Terms and Definitions, Need, Methodology, Considerations and Approaches.

Security Models: IA-CMM,ISM3, SSE-CMM: Importance, Usage, Structure and Architecture, Process Areas; Security Engineering and its need.

Security Standards and frameworks: ISO 27001: Evolution, Organizational Context, ISMS Implementation in Organizations; COBIT: Principles, Structure and Objectives.

Security Methodologies: IAM, IEM, OCTAVE, OSSTMM,SIPES.

Laws for Information Security: Introduction to The Indian IT Act, IPR, Patent law, Copyright Law.

Unit V : Security Audit/Assurance:

Security Audits : Need in Organizations, Auditor's responsibility, Types, Approaches, Technology- Based Audits : Penetration Testing and Vulnerability Scanning; Phases, Budgeting for Security Audits.

Privacy : Organizational implications, Practices ,Policy, Audits: Framework and Approach, Standards, Phases, Process : Design, Risk Analysis, Planning, Conducting, Reporting.

Text and Reference books:

[1] Nina Godbole, Information Systems Security-Security Management, Metrics, Frameworks and Best Practices, Wiley, 2009.

[2] Digital Forensics and Cyber Crime; Ibrahim Baggili; Springer.

[3] W. Kruse and J. Heiser, *Computer Forensics: Incident Response Essentials*, Massachusetts, Ed. Boston: Addision Wesley, 2001.

[4] Rick Ayers, Sam Brothers and Wayne Jansen : Guidelines on Mobile Device Forensics, NIST, 2014.