Cyber Security and Cyber Laws

Course Code: **MCA-253** **L T C**
Course Name: **Cyber Security and Cyber Laws** **3 1 4**

INSTRUCTIONS TO PAPER SETTERS:

1. Question No. 1 should be compulsory and cover the entire syllabus. There should be 10 questions of short answer type of 2.5 marks each, having at least 2 questions from each unit.
2. Apart from Question No. 1, rest of the paper shall consist of four units as per the syllabus. Every unit should have two questions to evaluate analytical/technical skills of candidate. However, student may be asked to attempt only 1 question from each unit. Each question should be of 12.5 marks, including its subparts, if any.
3. Examiners are requested to go through the Course Outcomes (CO) of this course and prepare the question paper accordingly, using Bloom's Taxonomy (BT), in such a way that every question be mapped to some or other CO and all the questions, put together, must be able to achieve the mapping to all the CO(s), in balanced way.

LEARNING OBJECTIVES:

In this course, the learners will be able to develop expertise related to the following:-

1. Fundamentals of cyber security and related safeguards.
2. Cyber threats and vulnerabilities.
3. Securing web applications.
4. Cyber Laws, Cyber Forensics and IPR.

PRE-REQUISITES:

Knowledge of computer basics and computer networks

COURSE OUTCOMES (COs):

After completion of this course, the learners will be able to:-

CO #	Detailed Statement of the CO	BT Level	Mapping to PO #
CO1	Demonstrate computer technologies, digital evidence collection, and reporting in forensic acquisition.	BTL2	PO1, PO2
CO2	Apply strategies of using information as a weapon and a target.	BTL3	PO1, PO2, PO3, PO5
CO3	Identify the principles of offensive and defensive information warfare for a given context.	BTL3	PO1, PO2, PO3, PO4, PO5, PO6, PO10
CO4	Analyze the social, legal and ethical implications of information warfare.	BTL4	PO1, PO2, PO3, PO4, PO5, PO6, PO10
CO5	Appraise key terms and concepts in cyber law, intellectual property and cyber crimes, trademarks, domain theft and Cyber Forensics.	BTL6	PO1, PO2, PO3, PO4, PO5, PO6, PO7, PO8, PO9, PO10, PO11

UNIT – I

No. of Hours: 10 **Chapter / Book Reference: TB1 [Chapters 1-3]**

Introduction to Cyber Security: Overview of Cyber Security, Internet Governance –

Challenges and Constraints

Cyber Threats: Cyber Squatting, Cyber Warfare, Cyber terrorism, Cybercrime, Cyber Offenses

Classification of Cybercrimes: Email spoofing, Spamming, Cyber defamation, Internet Time Theft, Data Diddling, Espionage, Hacking, Online Frauds, Computer Sabotage, Email Bombing, Computer Network Intrusion, Password Sniffing, Credit Card Frauds, Identify Theft

Cybercrime-Mobile and Wireless Devices: Proliferation of Mobile and Wireless Devices, Authentication Service Security, Attacks on Mobile Phones, Security Implications for Organizations, Measures for Handling Mobile Devices

Cyber Offenses: Categories, Attacks, Social Engineering, Cyber stalking, Botnets, Cloud Computing

UNIT – II

No. of Hours: 10 **Chapter / Book Reference: TB1 [Chapters 4-5]**

Cyber Security Vulnerabilities and Cyber Security Safeguards: Cyber Security Vulnerabilities-Overview, vulnerabilities in software, Proxy Servers and Anonymizers, Phishing, Password Cracking, Keyloggers and Spywares, Virus and Worms, Trojan Horse and Backdoors, Steganography, DoS and DDoS attacks, SQL Injection, Buffer Overflow, Attack on wireless Networks, Identity Theft (ID Theft)

UNIT – III

No. of Hours: 10 **Chapter / Book Reference: TB2 [Chapters 3-5]**

Securing Web Application, Services: Introduction, Basic security for HTTP Applications, Email Security, Back up Issues, Identity Management and Web Services, Authorization Patterns, Firewall

Intrusion Detection and Prevention System: Intrusion, Physical Theft, Abuse of Privileges, Access Management, Access management Models (DAC, OAC, RBAC), Unauthorized Access by Outsider, Malware infection, Intrusion detection and Prevention Techniques, Anti-Malware software, Network based Intrusion detection Systems, Network based Intrusion Prevention Systems, Host based Intrusion prevention Systems, Security Information Management, Network Session Analysis, System Integrity Validation

UNIT – IV

No. of Hours: 10 **Chapter / Book Reference: TB1 [Chapters 6,7,9,10]**

Cybercrime and Cyber Security: The Legal Perspective: Introduction, Cyber Security Regulations, Legal Landscape around the World, The Indian IT Act and Amendments, Digital Signatures and the Indian IT Act, Cyber Crime and Punishment

Understanding Computer Forensics: Cyber forensics and digital Evidences. Digital Forensics Life cycle, Network Forensics, Relevance of the OSI 7 layer model to Computer Forensics, Forensics and Social Networking Sites, Challenges in Computer Forensics, Forensics Auditing, Anti forensics

Intellectual Property in the Cyber Space: Copyrights, Jurisdiction Issues and Copyright Infringement, Multimedia and Copyright issues, WIPO, Intellectual Property Rights, Understanding Patents, Understanding Trademarks, Trademarks in