INSTITUTE OF AERONAUTICAL ENGINEERING
(Autonomous)
Dundigal - 500 043, Hyderabad, Telangana

COURSE CONTENT

CYBER LAWS AND SECURITY								
VI Semester: CSE								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
ACSD39	**Elective**	**3**	**0**	**0**	**3**	**40**	**60**	**100**
Contact Classes: 48	**Tutorial Classes: Nil**	**Practical Classes: Nil**				**Total Classes: 48**		
Prerequisite: Security Threats and Modelling								

I. COURSE OVERVIEW:
This course introduces the fundamentals of Cyber Laws and Cyber Security, focusing on the legal frameworks governing cyberspace and digital transactions. It covers the IT Act 2000, related legislations, intellectual property issues, and cybercrime. Students will also learn cybersecurity concepts, threat types, and organizational implications of cyber risks and social media misuse.

II.COURSES OBJECTIVES:
The student will try to learn:

I. The evolution of cyber law and its role in regulating cyberspace and digital communication.
II. The Information Technology Act, 2000 and its relevance to digital signatures, electronic records, and cybercrime.
III. The intersection of cyber law with intellectual property, civil, and criminal procedures.
IV. The cybersecurity threats, security models, and organizational challenges in managing cyber risks effectively.

III. COURSE OUTCOMES:
At the end of the course, students should be able to:

CO 1 Understand the foundational principles of cyber law and cyber jurisprudence.
CO 2 Interpret the key provisions of the Information Technology Act, 2000 and its practical implications.
CO 3 Analyze the legal intersections between cyber laws and IPR, civil, and criminal laws.
CO 4 Identify and classify various types of cyber threats and security breaches in networked environments.
CO 5 Evaluate organizational vulnerabilities and develop strategies to mitigate cyber risks.
CO 6 Assess ethical, legal, and social implications of cybercrime and cyberterrorism in global contexts.

IV. COURSE CONTENT:

MODULE-I: INTRODUCTION TO CYBER LAW (9)

Emergence of Cyber space. Cyber Jurisprudence, Jurisprudence and law, Doctrinal approach, Consensual approach, Real Approach, Cyber Ethics, Cyber Jurisdiction, Hierarchy of courts, Civil and criminal jurisdictions, Cyberspace-Web space, Web hosting and web Development agreement, Legal and Technological Significance of domain Names, Internet as a tool for global access.

MODULE-II: INFORMATION TECHNOLOGY ACT (10)

Overview of IT Act, 2000, Amendments and Limitations of IT Act, Digital Signatures, Cryptographic Algorithm, Public Cryptography, Private Cryptography, Electronic Governance, Legal Recognition of Electronic Records, Legal Recognition of Digital Signature Certifying Authorities, Cyber Crime and Offences, Network Service Providers Liability, Cyber Regulations Appellate Tribunal, Penalties and Adjudication.

MODULE-III: CYBER LAW AND RELATED LEGISLATION (10)

Patent Law, Trademark Law, Copyright, Software – Copyright or Patented, Domain Names and Copyright disputes, Electronic Data Base and its Protection, IT Act and Civil Procedure Code, IT Act and Criminal Procedural Code.

Relevant Sections of Indian Evidence Act, Relevant Sections of Bankers Book Evidence Act, Relevant Sections of Indian Penal Code, Relevant Sections of Reserve Bank of India Act, Law Relating To Employees And Internet, Alternative Dispute Resolution , Online Dispute Resolution (ODR).

MODULE-IV: INTRODUCTION TO CYBER SECURITY (10)

Basic Cyber Security Concepts, layers of security, Vulnerability, threat, Harmful acts, Internet Governance – Challenges and Constraints, Computer Criminals, CIA Triad, Assets and Threat, motive of attackers, active attacks, passive attacks, Software attacks, hardware attacks, Spectrum of attacks, Taxonomy of various attacks, IP spoofing, Methods of defence, Security Models, risk management, Cyber Threats-Cyber Warfare, Cyber Crime, Cyber terrorism, Cyber Espionage, etc., Comprehensive Cyber Security Policy.

MODULE-V: ORGANIZATIONAL IMPLICATIONS AND CYBERCRIME (9)

Introduction, cost of cybercrimes and IPR issues, web threats for organizations, security and privacy implications, social media marketing: security risks and perils for organizations, social computing and the associated challenges for organizations. Cybercrime and Cyber terrorism: Introduction, intellectual property in the cyberspace, the ethical dimension of cybercrimes the psychology, mindset and skills of hackers and other cyber criminals.

V.TEXT BOOK:

1. .K.Kumar," Cyber Laws: Intellectual property & E Commerce, Security", Dominant Publisher, 1st Edition, 2011.
2. Nina Godbole and Sunit Belpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley.

VI REFERENCE BOOKS:

1. Rodney D. Ryder, "Guide To Cyber Laws", Wadhwa and Company, New Delhi, 2nd Edition, 2007.
2. Vakul Sharma, "Handbook Of Cyber Laws" Macmillan India Ltd, 2nd Edition, PHI,2003.
3. B. B. Gupta, D. P. Agrawal, Haoxiang Wang, Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335, 2018.

VII. ELECTRONICS RESOURCES:

1. https://www.coursera.org/learn/intro-cyber-security
2. https://www.infosecawareness.in/
3. https://ipindia.gov.in/

VIII. MATERIALS ONLINE:

1. Course Outline Description
2. Tutorial question bank
3. Tech talk topics
4. Open-ended experiments
5. Definitions and terminology
6. Assignments
7. Model question paper – I
8. Model question paper – II
9. Lecture notes
10. . PowerPoint presentation
11. E-Learning Readiness Videos (ELRV)