



(Shri Ramkrishna Seva Mandal's)
ANAND COMMERCE COLLEGE

An Autonomous College (2025-26 to 2034-35)

(Affiliated to Sardar Patel University)

NAAC ACCREDITED 'A' GRADE (3.04 CGPA)

ISO 9001:2015

Syllabus as per NEP 2020 with effect from the Academic Year 2025-26



Bachelor of Commerce
B COM Semester – II

Course Code	UC02SECOM03	Title of the Course	Cyber Laws & Securities
Total Credit of Course	02	Hours Per Week	02

Course Objectives:	<ol style="list-style-type: none">1. Understand the basics of cyberspace and how the internet, cyber threats, and digital platforms work.2. Identify legal frameworks and recognize major laws governing cyber activities in India and globally.3. Apply security measures and will adopt safe practices for data privacy, cybersecurity and legal compliance.
--------------------	--

Course Content		
Unit	Description	Weightage* (%)
1.	Fundamentals of Cyberspace & Security Meaning of Cyberspace Basics of Internet & Digital World Introduction to Cyber Threats (Hacking, Phishing, Malware, Ransomware) Data Privacy & Protection and its Importance Digital Footprint & Online Identity Cyber Ethics & Responsible Use of Technology Cyberbullying, Social Media Risks, Dark Web Overview (Basic Awareness)	35%
2.	Laws of Cyber Laws (Legal Framework & Important Acts) Introduction to Cyber Law – Meaning, Need & Scope Information Technology (IT) Act, 2000 – Key Provisions Data Protection Laws – National & International Perspectives Cyber Contracts & Digital Signatures – Legal Validity Regulatory Authorities (CERT-In, IT Ministry, RBI Guidelines) Penalties & Offences under IT Act E-commerce & Cyber Law Privacy under Personal Data Protection Bill (latest)	35%

3.	Case Laws & Security Practices (Real Cases & Cyber Safety Tips) Landmark Cyber Crime Cases in India & Worldwide Prevention Strategies – How to Stay Safe Online Cyber Security Measures – Strong Passwords, Encryption, VPN Ethical Hacking & Role of Cyber Forensics Future Trends – AI, Blockchain, Cyberwarfare Basic Cyber Forensics Process Digital Evidence, Digital Arrests and Electronic Evidence Handling (Procedure and Legal Framework) Examples of Phishing Email (Case Studies)	30%
----	---	-----

Teaching-Learning Methodology	Class Room Teaching
--------------------------------------	---------------------

Internal and / or External Examination Evaluation

Sr. No.	Details of the Evaluation / Exam Pattern	50 Marks (%)	25 Marks (%)
1	Class Test (at least one)	15 (30%)	10 (40%)
2	Quiz (at least one)	15 (30%)	05 (20%)
3	Active Learning	05 (10%)	----
4	Home Assignment	05 (10%)	05 (20%)
5	Class Assignment	05 (10%)	----
6	Attendance	05 (10%)	05 (20%)
Total Internal (%)		50 (100%)	25 (100%)
College External Examination (%)		50 (100%)	25 (100%)

Course Outcomes: Having completed this course, the learners will be able to	
1.	Understand basics of cyberspace, digital identity and common cyber threats.
2.	Apply knowledge of cyber laws, IT Act, data protection and regulatory bodies.
3.	Demonstrate awareness of cybersecurity practices, ethics and future digital trends.

Suggested References:

Sr.No.	References
1	Viswanathan Suresh T.; The Indian Cyber Law with The Information Technology Act, 2000, Bharat Law House Pvt Ltd, New Delhi.
2	Varma Dr. Amita; Cyber Crime & Law, Central Law Publications, Allahabad.
3	Mishra Dr. J. P.; An Introduction to CYBER LAWS, Central Law Publications
Digital resources to be used if available as reference material	
1. CERT-In Reports (www.cert-in.org.in) – Government of India’s cyber incident updates.	
2. Interpol Cybercrime Resources (www.interpol.int) – Case studies and cyber law enforcement strategies.	
3. Stanford Cyber Policy Center (https://cyber.fsi.stanford.edu/) – Research on cyber law and governance	



**Chairman
BOS of Commerce
Anand Commerce College**



**Academic Coordinator
Anand Commerce College**



**Principal
Anand Commerce College**