Department – Commerce and Management

Aishwarya College (Autonomous)

Affiliated to Jai NarainVyas University, Jodhpur

NAAC "A" Grade,Recognised by UGC u/s 2(f) & 12 (B)

PG Diploma in Cyber Laws & Data Privacy

COURSE SCHEME

&

SYLLABUS

AISHWARYA COLLEGE OF EDUCATION (AUTONOMOUS)

Department of Commerce & Management - Course Name and Credit Scheme

PG DIPLOMA IN CYBER LAWS AND DATA PRIVACY - FIRST SEMESTER

NCrF Level	Sem	Course Type	Course Code	Course Name	H/W	Total Hours	Credits	CIA Marks	EoSE Marks	Max. Marks
6.5	I	DCC	CLFCC47001T	Cyber Laws & Its Fundamentals	6	90	6	20	80	100
		DCC	ITACC47001T	Information Technology Act & Allied Legislations	6	90	6	20	80	100
		DCC	CIECC47001T	Cybercrimes: Investigation, Enforcement and Prosecution	6	90	6	20	80	100
		DCC	ITECC47001T	ITContracts,E-Commerce and Legal Frameworks	6	90	6	20	80	100
		SEC	CSDCC47001T	Cyber-security & Sustainable Development	3	45	3	20	80	100
				Total Credits			**27**			

Post Graduate Diploma in Cyber Laws and Data Privacy (Semester-I)

Discipline Centric Core Course (DCC)

CLFCC47001T : Cyber Laws & Its Fundamentals

(20 CIA + 80 EoSE. = Max. Marks: 100)

Course Credits	No. of Teaching Hours Per Week	Total No. of Teaching Hours
6 Credits	6 Hours	90 Hours

Course Outcome: On successful completion of the course, the students will be able to:

- Developing thorough understanding of conceptual and theoretical foundations of cyber law.
- Understanding of the legall and scape governing cyber space
- Ability to identify and analyze cyber crimes in digital world.
- Developing awareness of jurisdictional and international legal issues.
- Awareness about recent trends and advancement in technology

SYLLABUS

Unit-I: Introduction to Cyber Law and Digital Society: Concept, Scope, Need and Importance of cyber law; Evolution of cyber law, Understanding Key Terminologies: Cybercrimes, cybersecurity, cyberspace etc., Jurisprudential foundation of cyber law, Cyber law and its relationship with Constitutional Law (Fundamental rights & Right to Privacy)

Unit-II: The Information TechnologyAct, 2000– Frame work and Governance: Objectives, Scope, Definitions under the Act: data, information, computer, computer resource, computer network, etc., Digital signatures and electronic records: Legal recognition and regulation, Certifying Authorities and the Controller, E-Governance and its legal framework, Key Provisions of the IT Act with landmark cases.

Unit-III: Cyber Crimes and Legal Remedies: Classification of cybercrimes, Legal provisions related to cybercrimes with landmark judgments, key provisions in Bhartiya Nayaya Sanhita, 2023 regarding cybercrimes, Investigation, Adjudication and Penalties, Cyber Cells and their role, CERT-IN and Enforcement Directorate, Jurisdiction and Enforcement Challenges in cyber crimes.

Unit-IV: Data Protection, Privacy & Surveillance Laws: Concepts of Data privacy, Overview- the Digital Personal Data Protection Act, 2023, Surveillance laws and privacy, Encryption and otherprivacy-preserving technologies, Legal challenges in implementing privacy-enhancing tools, Corporate responsibilities in data handling and breach.

Unit-V: Emerging Trends in Cyber Laws: Emerging Technologies, Generative AI, Block chain and Crypto currencies, IoT, Metaverse and Virtual Worlds, AI Powered Automation and Robotics, AI Driven Cyber Attacks, The Role of AI in law enforcement, Ethics and AI, Future of Cyber Law in the age of AI.

SUGGESTED BOOKS

1. Pavan Duggal, Cyber law: The Indian Perspective
2. Justice S. Ravindra, Right to Privacy:Constitutional DevelopmentinIndia
3. Information Technology Act, 2000 (Bare Act with Amendments)
4. Digital Personal Data Protection Act, 2023
5. Vivek Sood, Cyber Law Simplified
6. Articles from Journal of Cyber Law & Policy, Harvard Law Review, NUJS Law Review

Post Graduate Diploma in Cyber Laws and Data Privacy (Semester-I)

Discipline Centric Core Course (DCC)

ITACC47001T : Information Technology Act & Allied Legislations

(20 CIA + 80 EoSE. = Max. Marks: 100)

Course Credits	No. of Teaching Hours Per Week	Total No. of Teaching Hours
6 Credits	6 Hours	90 Hours

Course Outcome: On successful completion of the course, the students will be able to:

- Understand the legal framework governing information technology in India.
- Analyze the impact of the IT Act on various stake holders.
- Apply principles of data protection and privacy.
- Develop a critical understanding of emerging issues in information technology.
- Design strategies for compliance with the IT Act and other related legislations.

SYLLABUS

Unit-I: Introduction to Cyber Law and ITAct, 2000: Historical Background and Need for Cyber Law, Objectives and Scope of the IT Act, 2000, Key Definitions: Computer, Data, Electronic Record, Information, etc., LegalRecognition of Electronic Records and Signatures, Electronic Governance and Certifying Authorities

Unit-II: Offenses and Penalties under the IT Act: Overview of Cyber Crimes (Section 65–78), Hacking, Data Theft, Cyber Terrorism, Obscenity, Identity Theft, Phishing, etc., Intermediary Liability (Section79 and Safe Harbour Provisions), Cyber Appellate Tribunal and Adjudication Process, Investigation and Jurisdiction Issues in Cyber Crimes.

Unit-III: Regulatory Framework and Compliance : Role of Controller of Certifying Authorities, Digital Signature Certificates and Authentication, IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Due Diligence and Corporate Compliance.

Unit-IV: Allied Laws and Interface with Other Legislations: Indian Penal Code (IPC) and its Application to Cyber Crimes, Evidence Act, 1872 – Electronic Evidence and Admissibility, The Companies Act, 2013 – Data Governance Responsibilities, Data Protection Laws (comparison with GDPR), National Cyber Security Policy and CERT-IN Guidelines.

Unit-V: International Perspectives and Emerging Issues: International Cooperation and Model Laws (UNCITRAL, Budapest Convention), Cross- Border Data Flow and Jurisdiction Challenges, Role of WIPO in Cyber Intellectual Property Protection, E-Commerce and Consumer Protection, Case Studies on Global Cyber Law Disputes and Indian Jurisprudence.

SUGGESTED BOOKS

1. Justice Yatindra Singh–Cyber Laws
2. Vakul Sharma – Information Technology Law and Practice
3. Pavan Duggal– Cyber law– The Indian Perspective
4. Information Technology Act,2000 – Bare Act (with amendments)
5. Relevant Case Laws–Shreya Singhal v.Union of India etc.
6. Articles and Reports by UNODC, WIPO and OECD

Post Graduate Diploma in Cyber Laws and Data Privacy (Semester-I)

Discipline Centric Core Course (DCC)

CIECC47001T : Cybercrimes: Investigation, Enforcement and Prosecution

(20 CIA + 80 EoSE. = Max. Marks: 100)

Course Credits	No. of Teaching Hours Per Week	Total No. of Teaching Hours
6 Credits	6 Hours	90 Hours

Course Outcome: On successful completion of the course, the students will be able to:

- Gain practical knowledge of cyber crime investigation procedures.
- Develop skills to handle digital evidence ethically and legally.
- Enhance understanding of the challenges incombating cyber crimes.
- Be capable of formulating effective strategies for cyber crime prevention and enforcement

SYLLABUS

Unit-I: Overview of Cyber crimes: Definition, Origin and Evolution of Cybercrimes, Classification: Financial Crimes, Cyber Terrorism, Hate Speech, Obscenity, Cyberstalking, Online Harassment, etc., Cybercrime Trends: Ransomware, Deepfakes, Dark Web Activities, Victimology and Impact on Society.

Unit-II: Legal Frame work and Enforcement Mechanism: Provisions under the Information Technology Act, 2000, Relevant Sections of the IPC, Evidence Act, POCSO, and Special Laws, Role of Enforcement Agencies: Police, Cyber Crime Cells, CBI, NIA, CERT-IN, Jurisdiction, Investigation under CrPC (Sec 154–176) in Cyber Context, Mutual Legal Assistance Treaties (MLATs) and International Cooperation.

Unit-III: Investigation Techniques and Digital Evidence: Preliminary Inquiry and FIR in Cyber Offenses, Digital Evidence Collection, Preservation and Chain of Custody, Tools for Cyber crime Investigation: Packet Capture, Disk Imaging, Log Analysis, OSINT (Open Source Intelligence) and Dark Web Monitoring, Challenges in Investigating An onymized and Encrypted Communications.

UNIT-IV: Prosecution and Adjudication of Cyber Crimes: Drafting Charges and Framing Legal Strategy, Role of Prosecutors and Forensic Experts, Admissibility of Electronic Evidence (Section 65B of Evidence Act), Trial Process in Cybercrime Cases: Witness Examination, Cross-Examination, Expert Testimony.

UNIT-V: Issues, Challenges and Future Trends: Challenges in Cross-border Cybercrime Investigations, Cybercrime Against Women and Children: Legal Remedies, Use of Artificial Intelligence in Policing and Prosecution, International Best Practices and Future of Cyber Law Enforcement.

SUGGESTED BOOKS

1. Pavan Duggal– Cyber law & Cyber crime in India
2. Vakul Sharma– Cyber Crimes and Law
3. S.R.Sharma– Hand book of Cyber crime Investigation
4. Information Technology Act, 2000 (with Amendments)
5. Indian Evidence Act,1872–with focus on digital evidence
6. Government Guidelines: CERT-IN Advisories, Meit Y Notifications
7. Reports by UNODC, Interpol and NCRB

Post Graduate Diploma in Cyber Laws and Data Privacy (Semester-I)

Discipline Centric Core Course (DCC)

ITECC47001T : ITContracts, E-Commerce and Legal Frameworks

(20 CIA + 80 EoSE. = Max. Marks: 100)

Course Credits	No. of Teaching Hours Per Week	Total No. of Teaching Hours
6 Credits	6 Hours	90 Hours

Course Outcome: On successful completion of the course, the students will be able to:

- Ability to draft and review IT contracts in compliance with legal standards.
- Capacity to navigate the legall and scape of electronic transactions and digital signatures.
- Skills to address legal challenges in e-commerce business models.
- Awareness of international laws affecting online commerce.

SYLLABUS

Unit-I: Introduction to IT Contracts and E-Commerce: Nature and Evolution of E-Commerce, Types of E-Commerce Models: B2B, B2C, C2C,C2B, etc., Essential Elements of IT Contracts, Electronic Contracts: Types – Clickwrap, Browsewrap, Shrinkwrap, Formation and Validity of E-Contracts, Consent, Offer, and Acceptance in the Digital Realm.

Unit-II: Legal Recognition and Regulatory Framework: Legal Validity under the Information Technology Act, 2000, Digital Signatures and Electronic Authentication, Role of Certifying Authorities, UNCITRAL Model Law on E- Commerce, E-Transaction Rules under Indian and Global Law, RBI Guidelines and Consumer Protection (E-Commerce) Rules, 2020.

Unit-III: Contractual Obligations, Liability and Compliance: Drafting of IT Contracts (Software Development, SLA, NDAs, Licensing, Cloud Services), Liability of Intermediaries and Platform Operators, Terms of Service, Privacy Policies, and Return/Refund Policies, Breach of Contract, Remedies, and Limitation of Liability, Intellectual Property in Digital Transactions.

Unit-IV: Data Governance and Cyber security in E-Commerce: Data Protection and Privacy Obligations in Online Contracts, Cross-Border DataTransfer and Jurisdictional Issues, Impact of GDPR, Indian DPDP Act (if enacted) and IT Rules 2021, Cyber security Standards and Risk Management in E-Commerce, Fraud, Phishing and Consumer Protection.

Unit-V: Dispute Resolution and International Perspectives: Jurisdiction in Cross-Border E-Commerce Disputes, Online Dispute Resolution (ODR): Models and Practices, Arbitration Clauses in IT and E-Commerce Contracts, Role of ICANN, WIPO, and WTO in Digital Trade, International Case Studies: Amazon, Flipkart, Alibaba and Netflix Contractual Disputes.

SUGGESTED BOOKS

1. A. Ramaiya–Guide to the Companies Act (selected sections on IT Contracts)
2. R. Kishore & T.S.Mann– E-Commerce and Cyber Laws
3. Vakul Sharma – Information Technology Law and Practice
4. Pavan Duggal– E-Commerce Law in India
5. UNCITRAL Model Law on E-Commerce
6. Consumer Protection (E-Commerce) Rules, 2020
7. RBI Circulars & Guidelines –Relevant to online payments and KYC
8. WIPO & WTO Reports–On digital commerce and IPR

Post Graduate Diploma in Cyber Laws and Data Privacy (Semester-I)

Skill Enhancement Course (SEC)

CSDCC47001T : Cyber Security & Sustainable Development

(20 CIA + 80 EoSE. = Max. Marks: 100)

Course Credits	No. of Teaching Hours Per Week	Total No. of Teaching Hours
6 Credits	6 Hours	90 Hours

Course Outcome: On successful completion of the course, the students will be able to:

- Understand core cyber security concepts and their relevance to sustainable development
- Analyze the impact of cyber threats on SDGs
- Develop strategies for integrating cyber security measures into sustainable development projects
- Critically evaluate policies and frameworks promoting cyber security and sustainability

SYLLABUS

Unit-I: Introduction to Cyber security and Sustainable Development: Overview of cyber security principles and practices, Introduction to sustainable development and SDGs, The role of digital technology in achieving SDGs, Interlinkages between cyber security and sustainability, Case studies of digital initiatives for SDGs.

Unit-II: Cyber Threats and Risks in Sustainable Development: Types of cyber threats (malware, hacking, data breaches), Cyber vulnerabilities in critical infrastructure(energy,water,health),Impact ofcyber incidentsonsustainabledevelopment projects, Risk assessment and management

Unit-III: Protecting Digital Infrastructure for Sustainable Development: Cyber security strategies and best practices, Secure design of digital systems and IoT devices, Role of encryption, authentication and access controls, Public-private partnerships and cybersecurity governance.

Unit-IV: Policy, Governance and Ethical Issues: National and international cyber security policies, Ethical considerations in digital sustainability, Data privacy and humanrights, Policy frameworks supporting SDGs and cyber security.

Unit-V: Cyber security for Sustainable Development Goals: Case studies linking cyber security initiatives with SDGs (e.g. health, education, climate), Innovations and emerging technologies (AI, blockchain) in SDGs, Challenges and future directions.

SUGGESTED BOOKS

1. "Cyber security and Sustainable Development" by Jane Doe (2022)
2. "Digital Infrastructure and SDGs" by John Smith (2021)
3. Reports from UN and ITU on cyber security and sustainable development