



# Sunrise University

Approved by Govt. of Rajasthan vide Sunrise University Act, 2011  
Recognized by UGC Act, 1956 u/s 2 (f)

## POST GRADUATE DIPLOMA IN LABOUR LAW ONE YEAR SCHEME

PAPERS CODE	PAPERS NAME	INTERNAL	EXTERNAL	TOTAL
PGDCL-101	Basics of Computer, Internet and Cyber World	40	60	100
PGDCL -102	Information Technology Law	40	60	100
PGDCL -103	Cyber-Crimes & Forensics	40	60	100
PGDCL -104	Cyber Security in E-Commerce	40	60	100
PGDCL -105	IPR in Cyber World	40	60	100
PGDCL -106	Investigation of Cyber Crimes	40	60	100
Total		240	360	600

**SunRise**  
**UNIVERSITY**  
**ALWAR**



## PGDCL-101 Basics of Computer, Internet and Cyber World

### **Course Objectives:**

1. Acquainting the students with basics computers.
2. Understanding the uses of internet.
3. Providing extensive knowledge regarding the types of network.
4. Providing general understanding of email and domain system.
5. Providing basic knowledge about the Emerging Cyber Concepts.

### **Course Outcomes:**

1. The student knows about the basic concepts relating to computers.
2. The student has elementary knowledge about computer hardware and software.
3. Knowledge of operating system.
4. Knowledge regarding types of network.
5. Awareness about emerging cyber concepts.

### **Unit 1**

1. History of Computers, Areas of Application
2. Computers and its Components, Hardware, Hard disk, SD Card
3. Computer Software: Application Software and System Software

### **Unit 2**

1. Concept of Operating System
2. Business Data Processing
3. Networks and internet, Types of Network.

### **Unit 3**

1. Search Engines, E –mails and WWW
2. Internetworking Devices, Internet Service Provider, IP Address
3. Communication Protocols and Wireless Networks

### **Unit 4**

1. Working of Email System, Domain Name, Blogs,
2. Social Media
3. Emerging Cyber Concepts: Cloud Computing

### **REFERENCE READINGS:**

1. Sinha, Priti and Sinha, Pradeep K. (2004) Computer Fundamentals, BPB Publications
2. Seth, Karnika (2016), Computers, Internet And New Technology Laws-A Comprehensive Reference Work With Special Focus On Developments In India, Lexis Nexis
3. Paar, Christofand Pelzl, Jan (2011), Understanding Cryptography: A Textbook for Students and Practitioners, Springer
4. Hassall (2002) Multimedia Communications: Applications, Networks, Protocols and Standards, Pearson Education India
5. Rao, Raga Surya (2017). Lectures on Cyber Law, Gogia Law Agency.



## PGDCL -102 Information Technology Law

### Course Objectives:

1. Concepts of Technology and Law
2. Providing elementary understanding the authorities under IT Act
3. Penalties & Offences under IT Act
4. Cyber Space Jurisdiction
5. Scope of Cyber Laws.

### Course Outcomes:

1. The student is able to understand the technicalities of law in Cyber World.
2. Extensive knowledge regarding jurisdictional issues in IT Act.
3. Various important national and international cyber laws.
4. Understands the scope of Cyber Law
5. The students is able to understand the basic concept of International Technology

### Unit 1

1. Information Technology: Understanding the Basic concepts
2. Evolution of the IT Act 2000, Genesis and Necessity
3. Nature, Scope and Importance of IT Act

### Unit 2

1. Salient features of the IT Act, 2000,
2. Electronic records and Digital Signature
3. Regulation of Certifying Authorities

### Unit 3

1. Duties of Subscribers
2. The Cyber Regulation Appellate Tribunal

### Unit 4

1. Offences & Penalties under IT Act
2. Investigation Officer & their power under IT Act

### REFERENCE READINGS:

1. Rattan, Jyoti and Rattan, Vijay (2019) Cyber Laws & Information Technology, Bharat Law House Pvt Ltd
2. Padmavati, L. (2015) Lectures on Cyber Laws [Information Technology Act, 2000], Asia Law House
3. Gupta, Apar (2015) Commentary On Information Technology Act– With Rules, Regulations, Orders, Guidelines, Reports And Policy Documents, Lexis Nexis
4. Duggal, Pavan (2017) Cyber Law - An exhaustive section wise Commentary on the Information Technology Act along with Rules, Regulations, Policies, Notifications etc., Universal Law Publishing - an imprint of LexisNexis
5. Nappanee, N.S. (2017) Technology Laws Decoded, Lexis Nexis.



## **PGDCL -103 Cyber-Crimes & Forensics**

**Objective:** The paper aims to create the basic clarity and understanding of cybercrimes and cyber security laws to the professionals learning the ethical hacking programme. The paper would address and emphasize on the activities leading to infringement of individual or organizational privacy. Further, the paper intends to create highly sensitized professionals who can be responsible for handling the cyber security issues pertaining to varied domains and dealing in forensics diligently.

---

### **Unit I: Introduction to Cyberspace, Cybercrime and Cyber Law**

The World Wide Web, Web Centric Business, E Business Architecture, Models of E Business, E Commerce, Threats to virtual world. Cyber Crimes & social media, Cyber Squatting, Cyber Espionage, Cyber Warfare, Cyber Terrorism, Cyber Defamation. Online Safety for women and children, Misuse of individual information. Objectives, Applicability, Non applicability and Definitions of the Information Technology Act, 2000.

### **Unit II: Regulatory Framework of Information and Technology Act 2000**

Digital Signature, E Signature, Electronic Records, Electronic Evidence and Electronic Governance. Controller, Certifying Authority and Cyber Appellate Tribunal. (Rules announced under the Act)

### **Unit III: Offences and Penalties**

Offences under the Information and Technology Act 2000, Penalty and adjudication. Punishments for contraventions under the Information Technology Act 2000 (Case Laws, Rules and recent judicial pronouncements to be discussed). Limitations of Cyber Law.

### **Unit IV: Fundamentals of Cyber Forensics**

Cyber Forensic Basics- Introduction to Cyber Forensics, Storage Fundamentals, File System Concepts, Data Recovery, Operating System Software and Basic Terminology Data and Evidence Recovery- Introduction to Deleted File Recovery, Formatted Partition Recovery

### **Unit V: Data Recovery Tools, Data Recovery Procedures and Ethics**

Gathering Evidence- Precautions, Preserving and safely handling original media for its admissibility, Document a Chain of Custody and its importance, Complete time line analysis of computer files based on file creation, file modification and file access, Recover Internet Usage Data, Data Protection and Privacy, Recover Swap Files/Temporary Files/Cache Files, Introduction to Encase Forensic Edition, Forensic Toolkit etc, Use computer forensics software tools to cross validate findings in computer evidence-related cases.

### **Unit VI: Cyber Forensics Investigation**

Introduction to Cyber Forensic Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Encryption and Decryption methods, Search and Seizure of Computers, Recovering deleted evidences, Password Cracking, Cracking with GPU Systems, Hashcat. Work on open Source, Commercial tools and Cyber range.

### **REFERENCE READINGS:**

1. Craig, B. Cyber Law: The Law of the Internet and Information Technology. Pearson Education
2. Paintal, D. Law of Information Technology. New Delhi: Taxmann Publications Pvt. Ltd.
3. Lindsay, D. (2007). International domain name law: ICANN and the UDRP. Oxford: Hart Publishing.
4. Sharma J. P, & Kanojia S. (2016). Cyber Laws. New Delhi: Ani Books Pvt. Ltd.
5. Duggal, P. Cyber Laws. (2016) Universal Law Publishing.



## PGDCL -104 Cyber Security in E-Commerce

### Course Objectives:

1. Acquainting the students with Cyber Security, Data Privacy and Data Protection.
2. Providing an elementary understanding of the Types of Security threats.
3. Providing extensive knowledge regarding, Ethical Hacking, Email security: web authentication.
4. To make the student understand the E-commerce and its application.
5. To make the student understand the Electronic Contract.

### Course Outcomes:

1. The student understands the concept and process of cyber security.
2. The student understands the Online Dispute Resolution.
3. The student knows how to apply Network & Mobile Security Techniques.
4. The student understands issues in e-commerce.
5. The student knows about E-Commerce and E-Business-Models and Approaches.

### Unit 1

1. Cyber Security: Meaning and Scope
2. Computer & Cyber Security: (a) Types of Attacks, (b) Types of Security threats, (c) Hacking Techniques

### Unit 2

1. Database Security; Operating System Security
2. Advance Computers, Network & Mobile Security Techniques
3. Security issues: debit cards, credit cards, ATM, Secure Electronic Transactions

### Unit 3

1. Online Business: Definition of E-Commerce, Types of E-Commerce, Important issues in Global E-commerce
2. Laws relating to E-Commerce, Intellectual Property Rights, International Trade Law

### Unit 4

1. E-Commerce: E-banking, Online Payment gateways, Electronic Cheques in India
2. Electronic Contract: Meaning, Types and Formation of e-contracts

### REFERENCE READINGS:

1. Sharma, Pankaj (2013). Information Security and Cyber Laws, S.K. Kataria & Sons
2. Bhushan Rathore Jamshed (2017). Fundamentals of Cyber Security, BPB
3. Raef, Meeuwisse (2017). Cyber-security for Beginners, Cyber Simplicity Ltd
4. Dhawan, Nidhi (2017). A Handbook of E-commerce, Sun India Publications
5. Gupta, Pralok (2020). E-Commerce in India: Economic and Legal Perspectives, Sage Publications India Pvt. Ltd.



## PGDCL -105 IPR in Cyber World

### Course Objectives:

1. Acquainting the students with Intellectual Property Rights
2. Providing an elementary understanding of the Digital Environment
3. Providing an elementary understanding of Copyright Issues in Cyber World and Protecting Trademarks in Digital Environment.
4. Providing knowledge regarding protection of trademarks in Digital Era.
5. To understand the concepts of Patent in Cyber world.

### Course Outcomes:

1. The student understands the scope of IPR issues in cyber world.
2. The student knows in detail about important national and international conventions.
3. The student is aware of the provisions relating to IPR in cyber world.
4. The student has a broad understanding of the application of IPR to Computer Technology
5. The student knows about the protection of Copyright in Digital Environment.

### Unit 1

1. International Conventions on Copyright, Berne Convention, WIPO Treaty
2. Scope of Copyright protection in the digital environment

### Unit 2

1. Concept of Trademarks in Internet Era
2. Jurisdiction in Trademark Disputes
3. Protecting Trademarks in Digital Environment

### Unit 3

1. International Conventions on Patents
2. Provisions of Patent Act 1970 in relation to cyber world
3. Procedure of Patenting relating to digital technology

### Unit 4

1. IPR Issues: Challenges, Settlement of Disputes
2. Uniform Dispute Resolution Policy
3. Legal framework: National & International level

### REFERENCE READINGS:

1. Unni, V.K. (2005) Trade Mark and the Emerging Concepts of Cyber Property Rights, Eastern Law House
2. Duggal, Pavan (2014) Legal Framework on Electronic Commerce and Intellectual Property Rights in Cyberspace, Universal Law Publishing - An imprint of Lexis Nexis
3. Falls, Michaela (2011) Understanding Developments in Cyberspace Law: Leading Lawyers on Examining Privacy Issues, Addressing Security Concerns, and Responding to Recent it Trends (Inside the Minds), West Publishing Co
4. Saha, Subhasis (2012) Challenges to Intellectual Property Rights in Cyberspace, LAP Lambert Academic Publishing



## PGDCL -106 Investigation of Cyber Crimes

### Course Objectives:

1. Acquainting the students with Cyber Crimes
2. Providing an elementary understanding of the Investigation of Cyber Crimes.
3. Making the student comprehend the working of various Agencies for investigation of cyber-crimes in India,
4. Making the student aware of Digital Evidences.
5. To understand the different aspects of cyber forensic.

### Course Outcomes:

1. The student has better knowledge of Cyber Crimes.
2. The student has competence to understand the procedure of investigation of cyber crime.
3. The student knows the power and functions of investigating agency.
4. The student knows the importance of digital evidence.
5. The student has better ability and skills to deal with Cyber-Crimes.

### Unit 1

1. Classification of Cyber Crimes: Hacking, Obscenity, Software piracy
2. Difference between traditional crimes & cyber crime
3. Factors responsible for cyber crimes

### Unit 2

1. Cyber Criminal Mode
2. Investigation of Cyber Crimes
3. Investigation of malicious applications

### Unit 3

1. Various agencies for investigation of cyber crimes in India
2. Powers & functions of investigating agencies
3. Procedures followed by first responders

### Unit 4

1. Application of forensic science in cyber world
2. Forensic techniques (a) Computers Forensics (b) Mobile Forensic (c) Forensic Tools
3. Anti-Forensics

### REFERENCE READINGS:

1. Blitz (2011) Computer Forensics and Cyber Crime: An Introduction, Pearson Education India
2. Staniforth, Andrew and Akhgar, Babak (2017) Blackstone's Handbook of Cyber Crime Investigation,
3. Marcella Jr., Albert (2007) Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Second Edition (Information Security), Auerbach Publications
4. Reyes, Anthony and Brittson, Richard (2007) Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors, Syngress
5. Reddy, Niranjan (2019) Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations, Apress.



# Sunrise University

Approved by Govt. of Rajasthan vide Sunrise University Act, 2011  
Recognized by UGC Act, 1956 u/s 2 (f)



**SunRise**  
**UNIVERSITY**  
**ALWAR**