MAHARSHI DAYANAND UNIVERSITY, ROHTAK
DEPARTMENT OF LAW

PG
DIPLOMA
IN
CYBER LAW

Session 2024-25

P.G. Diploma in Cyber Law

P.G. Diploma in Cyber Law is 1- year postgraduate course involving issues related to the internet, communication technology, including knowledge relating to cyber jurisprudence, E-commerce and Cyber Security.

1. Program Outcomes

PO1-Knowledge of Cyber World and Cyber Law in general

PO2-The various aspects of cyber crimes

PO3-Understanding the problems relating to e-commerce and taxation

PO4-Intellectual Property issues in IT Act

PO5-International Perspective in Cyber Law

2. Eligibility

Bachelor/Master degree with at least 45% marks (42.75% marks for SC/ST/Blind/Visually and Differently Abled candidates of Haryana only) in aggregate or any other examination recognized by M.D. University, Rohtak as equivalent thereto.

3. Intake Proposed and Seat Distribution as Per Reservation Policy

Name of Programme	AIO	HOGC	SC	Deprived SC	BC (A)	BC (B)	DA/ PwD/ PH/ESM/ DFF	EWS	No. of sanctioned seats
P.G. Diploma in Cyber Law									30

Total No. of seats 30

Reservation Policy will be followed as per State Government and M.D. University Norms.

4. Proposed Fees

30,000/- for Diploma in Cyber Law

5 Scheme of the Examination

There shall be internal as well as semester end examination. The examination shall comprise of 100 marks in each course/Paper out of which 70 marks are for theory and 30 marks are for internal assessment.Internal Assessment 30 Marks (20 Marks Sessional Examination, 5 Marks Assignment/Seminars presentations and 5 Marks Attendance)

Note: The course comprises of Two Semesters: Semester I is of 24 credits and semester II is of 24 credits.

Revised Programme Structure for the PG Diploma in Cyber Law

	Semester	Discipline Specified Course (DSC)	Skill Enhancement Courses (SEC)/ Vocational Courses (VOC)/Internship	Dissertation	Total Credits
Student should select any one option					
Diploma Program (Both Semester 1 and Semester 2)					
Option I	**I**	Cyber Jurisprudence	Internship (3 weeks)*		**24**
		Basics of Computer, Internet and Cyber World			
		Information Technology Law			
		Cyber-Crimes			
		E-Governance			
	II	Cyber Security in E-Commerce	Internship (3 weeks)*		**24**
		IPR in Cyber World			
		Investigation of Cyber Crimes			
		E-Commerce and Taxation			
		International Cyber Law			

*Minimum 120 hours shall be completed in internship.

Semester-I:

Sr. No.	Name of Paper	Code	Written	Internal	Total marks	Time
1.	Cyber Jurisprudence	24LAWC101DS01	70	30	100	3 Hrs
2	Basics of Computer, Internet and Cyber World	24LAWC101DS02	70	30	100	3 Hrs
3	Information Technology Law	24LAWC101DS03	70	30	100	3 Hrs
4	Cyber-Crimes	24LAWC101DS04	70	30	100	3 Hrs
5	E-Governance	24LAWC101DS05	70	30	100	3 Hrs
6	*Internship/Project Report	24LAWC101IN01	100 Marks (70 marks for Internship Report and 30 marks for presentation before committee			

*The student has to undergo an internship for 3 weeks for Skill Enhancement with the organization/Firm/Unit, advocate in the concerned field. On completion of the internship, the student has to produce a certificate from such organization/Firm/Unit or advocate or expert person in the concerned field to the effect that he/she has completed the internship. The student has to prepare a detailed internship report which will carry 70 marks. The Viva-Voce Examination/Presentation of the report for 30marks shall be conducted by a committee of three examiners consisting of HOD/his nominee, teacher concerned and one external examiner.

Semester-II:

Sr. No.	Name of Paper	Code	Written	Internal	Total marks	Time
1.	Cyber Security in E-Commerce	24LAWC102DS01	70	30	100	3 Hrs
2.	IPR in Cyber World	24LAWC102DS02	70	30	100	3 Hrs
3.	Investigation of Cyber Crimes	24LAWC102DS03	70	30	100	3 Hrs
4	E-Commerce and Taxation	24LAWC102DS04	70	30	100	3 Hrs
5	International Cyber Law	24LAWC102DS05	70	30	100	3 Hrs
6	*Internship/Project Report	24LAWC102IN01	100 Marks (70 marks for Internship Report and 30 marks for presentation before committee			

*The student has to undergo an internship for 3 weeks for Skill Enhancement with the organization/Firm/Unit, advocate in the concerned field. On completion of the internship, the student has to produce a certificate from such organization/Firm/Unit or advocate or expert person in the concerned field to the effect that he/she has completed the internship. The student has to prepare a detailed internship report which will carry 70 marks. The Viva-Voce Examination/Presentation of the report for 30 marks shall be conducted by a committee of three examiners consisting of HOD/his nominee, teacher concerned and one external examiner.

*Minimum 120 hours shall be completed in internship.

SEMESTER- I
PAPER-1

Program Name	PGDiploma in Cyber Law	Program Code	
Course Name	Cyber Jurisprudence	Course Code	24LAWC101DS01
Course Credits	4	No. of hours/Week	4
Duration of End term examination	3 hours	Max. marks	100 Theory - 70 Marks (External) and 30 Marks (Internal)].

Note: The syllabus is divided in four units. The Examiner will set nine questions in all. First eight questions will be set by taking two questions from each unit. Question no. nine will consist of seven parts from all four units. The students have to attempt five questions in all selecting one question each from unit-I to IV. Question no. nine will be compulsory.

Learning Objectives:
1. Student will be acquainted with sources, hierarchy and innovative mechanism on cyber jurisprudence
2. Students will learn about cyber space, it's jurisdiction and interface between technology and law
3. Students will understand of issues of security and privacy with technical issues in cyber contracts.
4. Students will know about software development, licensing agreement and drafting of cyber contracts.
5. Students will have acquaintance with basic concepts of cyber jurisprudence and practical aspects of drafting of cyber contracts

Learning Outcomes:
1. Students become familiar with hierarchy of courts and their procedure.
2. Students will get equipped with knowledge of technology as well as jurisdictional aspect in the cyber space.
3. Students will be able to identify issues pertaining to privacy and security and to resolve such issues.
4. Students will develop their understanding regarding licensing issues and compliance of legal requirements.
5. Students will be able to know about the scope of privacy in the digital era.

Unit 1
1. Meaning and Sources of cyber Law.
2. Hierarchy & Composition of the Indian Judiciary
3. Civil Court Structure and Procedures
4. Criminal Court Structure and Procedures
5. Alternate Means of Dispute Resolution / ODR

Unit 2
1. Understanding of Cyber Space
2. Interface of Technology and Law
3. Internet Governance,
4. Jurisdiction in Cyber Space

Unit 3
1. Issues relating to Security
2. Issues relating to Privacy
3. Technical Issues involved in Cyber Contracts

Unit 4
1. Non-Disclosure Agreements
2. Software Development &Licencing Agreements
3. Drafting of Cyber Contracts

REFERENCE READINGS:
1. Kumar, Hiren, Sarma Deva, Dutta Nitul, Jadav Nilesh, Pricop Emil (2021), Cyber Security: Issues and Current Trends, Springer Publications
2. Seth, Karnika (2021), Computers, Internet and New Technology Laws-A comprehensive reference work with special focus on developments in India, Lexis Nexis
3. Khanna, Sri Ram (2018), Digital Drive E-governance and Internet Services in India, New Century Publications
4. Malik, Krishan Pal (2023), Information Technology & Cyber Law, Allahabad Law Agency
5. Rodney D Ryder & Naren Nikhil (2020), Internet Law, Bloomsbury

Program Name	P.G. Diploma in Cyber Law	Program Code	
Course Name	Basics of Computer, Internet and Cyber World	Course Code	24LAWC101DS02
Credits	4	No. of hours/Week	4
Duration of End term examination	3 hours	Max. marks	100 Theory - 70 Marks (External) and 30 Marks (Internal)].

Note: The syllabus is divided in four units. The Examiner will set nine questions in all. First eight questions will be set by taking two questions from each unit. Question no. nine will consist of seven parts from all four units. The students have to attempt five questions in all selecting one question each from unit-I to IV. Question no. nine will be compulsory.

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

Learning Outcomes:
1. Knowledge about the basic concepts relating to computers.
2. Knowledge of Elementary issues 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 of Computer.
2. Computer and its Components:Hardware, Hard disk, SD Card
3. Computer Software: Software Application 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. Seth, Karnika (2016), Computers, Internet And New Technology Laws-A Comprehensive Reference Work With Special Focus On Developments In India, Lexis Nexis
2. Halsall (2002) Multimedia Communications: Applications, Networks, Protocols and Standards, Pearson Education India
3. Paar, Christofand Pelzl, Jan (2011), Understanding Cryptography: A Textbook for Students and Practitioners,Springer
4. Rao, Rega Surya (2017). Lectures on Cyber Law,Gogia Law Agency
5. Sinha, Priti and Sinha, Pradeep K. (2004) Computer Fundamentals, BPB Publications

Program Name	P.G. Diploma in Cyber Law	Program Code	
Course Name	Information Technology Law	Course Code	24LAWC101DS03
Credits	4	No. of hours/Week	4
Duration of End term examination	3 hours	Max. marks	100 Theory - 70 Marks (External) and 30 Marks (Internal)].

Note: The syllabus is divided in four units. The Examiner will set nine questions in all. First eight questions will be set by taking two questions from each unit. Question no. nine will consist of seven parts from all four units. The students have to attempt five questions in all selecting one question each from unit-I to IV. Question no. nine will be compulsory.

Learning Objectives:
1. Concept of Technology and Law
2. Providing elementary understanding the Authorities under IT Act, 2000
3. Penalties & Offences under IT Act, 2000
4. Cyber Space Jurisdiction
5. Scope of Cyber Laws.

Learning Outcomes:
1. The student will be able to understand the technicalities of law in Cyber World.
2. The student will be able to understand extensive knowledge regarding jurisdictional issues in IT Act.
3. The student will be able to understand various important national and international cyber laws.
4. The student will be able to understand the scope of Cyber Law
5. The students will be able to understand the basic concept of International Technology

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

Unit 2
1. Salient features of the complete 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, 2000
2. Investigation Officer & their power under IT Act, 2000

REFERENCE READINGS:
1. 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
2. Gupta, Apar (2015) Commentary On Information Technology Act– With Rules, Regulations, Orders, Guidelines, Reports And Policy Documents, Lexis Nexis
3. Nappinai, N.S. (2017) Technology Laws Decoded, Lexis Nexis
4. Padmavati, L. (2015) Lectures on Cyber Laws [Information Technology Act, 2000],Asia Law House
5. Rattan, Jyoti and Rattan, Vijay (2019) Cyber Laws & Information Technology, Bharat Law House Pvt Ltd

Program Name	P.G. Diploma in Cyber Law	Program Code	
Course Name	Cyber-Crimes	Course Code	24LAWC101DS04
Credits	4	No. of hours/Week	4
Duration of End term examination	3 hours	Max. marks	100 Theory - 70 Marks (External) and 30 Marks (Internal)].

Note: The syllabus is divided in four units. The Examiner will set nine questions in all. First eight questions will be set by taking two questions from each unit. Question no. nine will consist of seven parts from all four units. The students have to attempt five questions in all selecting one question each from unit-I to IV. Question no. nine will be compulsory.

Learning Objectives:
1. Acquainting of the students with the Cyber Crimes.
2. Providing of the necessary understanding about freedom of speech in cyber space to the students.
3. Providing about the understanding of Issues in Internet Governance.
4. To understand the various International Organizations.
5. To understand Social Media and its Role in Cyber World.

Learning Outcomes:
1. Understanding of the elements of cybercrime and how to deal with such issues with clarity in theory as well as in practical aspects.
2. The studentswill be able to understand the Prevention of Cyber Crimes.
3. The students will be able to knows various legal provisions of cyber-crimes and the mechanism of their enforcement.
4. The students will be able to knows the essential legal provisions of internet-governance.
5. The students will acquire the understanding of Internet

Unit 1
1. Meaning of Cyber Crimes, issues and Computer related crimes
2. History, Development and Reasons for Growth of Cyber Crimes
3. Social Media and its Role in Cyber World, Fake News, Defamation

Unit 2
1. Prevention of Cyber Crimes
2. Critical analysis of the IT Act, 2000
3.International position on Free Speech on Internet

Unit 3
1. Cyber Crimes: Obscenity, Stalking, Hate Speech
2. Data Theft Hacking, Phishing
3. Sedition, Privacy, Cyber-terrorism

Unit 4
1. Cyber Law: International Perspective, Budapest Convention on Cyber Crime
2. Social Networking sites vis-à-vis Right to privacy

REFERENCE READINGS:
1. Arora, Sushma and Arora, Raman (2018) Cyber Crimes and Laws, Taxmann
2. Fatima, Talat (2016) Cyber Crimes, Eastern Book Company
3. Indian Institute of Banking and Finance (2017) Prevention of Cyber Crimes and Fraud Management,Macmillan Publishers India Private Limited
4. Jain, Ashok K. (2019) Cyber Law, Ascent Publication
5. Krishna, A. Gopala (2019) Cyber Crime and Cyber Laws,Prowess Publishing

Program Name	Diploma in Cyber Law	Program Code	
Course Name	E-Governance	Course Code	24LAWC101DS05
Credits	4	No. of hours/Week	4
Duration of End term examination	3 hours	Max. marks	100 Theory - 70 Marks (External) and 30 Marks (Internal)].

Note: The examiner has to set a total of nine questions (two from each unit and one compulsory question consisting of short answer from all units. The candidate has to attempt one question each from each unit along the compulsory question (5 x 14 = 70 marks)

Course Objectives:
1. Students will be acquainted with rights needs, scope and components of E-Governance.
2. Students will learn about Introduction National e-Governance Plan that is NeGP.
3. Students will know about the E-Governance initiative in Haryana.
4. Students will have insight into the role of IT in Justice Delivery System.
5. Students will have acquaintance with basic and practical aspects of E-governance Strategies.

Course Outcomes:
1. Students become familiar with the concept of E-Governance and its major components.
2. Students will get equipped with knowledge of framework for national E-Governance.
3. Students will be able to understand the actions taken by government of Haryana to strengthen the administration by E-Governance.
4. Students will become familiar with adoption of E-governance in functioning of courts.
5. Students will be able to understand the functioning of E-Governance in present scenario.

Unit 1
1. Needs, Scope and components of E-Governance.
2. Evolution of E-Governance and present global trends in E- governance
3. Area of E-Governance and Issues in E-governance
4. Role of Social Media in E-Governance

Unit 2
1. Introduction to NeGP (National e-Governance Plan)
2. The framework for e- Governance
3. National e-Governance strategy
4. Capacity Building initiatives under NeGP

Unit 3
1. E-Governance initiative in Haryana
2. CM Window
3. Public Health Engineering Department Haryana
4. National Rural Health Mission Haryana
5. Social Justice and Empowerment Department

Unit 4
1. Automation of Case Management Processes
2. Provision of online services.
3. Establish information gateways between courts and government agencies
4. Creation of National Judicial Data Grid agencies.

REFERENCE READINGS:
1. C.S.R.Prabhu : E-Governance: Concepts and Case Studies, Prentice Hall of India Pvt. Limited (2004).
2. Backus, Michiel : E-Governance in Developing Countries, IICD Research Brief, No. 1 (2001)
3. Information Technology & Cyber Law, Dr. Krishna Pal malik, (Allahabad Law Agency, 2023)
4. E-Governance in India: Problems, Prototypes and Prospects, Puneet Kumar (Nova Publisher, 2016)
5. **E-Governance in India**: **Interlocking politics, technology and culture,** Bidisha Chaudhuri, (Routledge, 2014)

Program Name	P.G. Diploma in Cyber Law	Program Code	
Course Name	*Internship	Course Code	24LAWC101IN01
Credits	4	No. of hours/Week	3
Duration of End term examination	---	Max. marks	100 Marks (70 marks for Internship Report and 30 marks for presentation before committee)

Learning Objectives:
1. Acquainting to the students with practical aspects in the concerned field.
2. Providing to the students an opportunity to work with expert in the concerned field.
3. Providing the students a chance to develop clarity of law in practice.
4. To make the students to understand the working of the practitioners in the concerned field.
5. To make the students competent to deal with the issues and problems of the victims and help them with a professional approach.

Learning Outcomes:
1. The students will be able to knows about the concerned subject in practical sense.
2. The students will be more efficient in dealing with problems in the area.
3. The students will be able in builds up a professional approach in helping the victims/clients.
4. The students will be able toevolve in the relevant area with complete understanding of subjects.
5. The student will be more pro-active in expanding his legal and social understanding of the laws.

*The student has to undergo an internship for 3 weeks for Skill Enhancement with the organization/Firm/Unit, advocate in the concerned field. On completion of the internship, the student has to produce a certificate from such organization/Firm/Unit or advocate or expert person in the concerned field to the effect that he/she has completed the internship. The student has to prepare a detailed internship report which will carry 70 marks. The Viva-Voce Examination/Presentation of the report for 30 marks shall be conducted by a committee of three examiners consisting of HOD/his nominee, teacher concerned and one external examiner.

Semester-II

Program Name	P.G. Diploma in Cyber law	Program Code	
Course Name	Cyber Security in E-Commerce	Course Code	24LAWC102DS01
Credits	4	No. of hours/Week	4
Duration of End term examination	3 hours	Max. marks	100 Theory - 70 Marks (External) and 30 Marks (Internal)].

Note: The syllabus is divided in four units. The Examiner will set nine questions in all. First eight questions will be set by taking two questions from each unit. Question no. nine will consist of seven parts from all four units. The students have to attempt five questions in all selecting one question each from unit-I to IV. Question no. nine will be compulsory.

Learning Objectives:
1. Acquainting of the studentswithCyber 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 studentsto understand theE-commerce and its application.
5. To make the studentsto understand the Electronic Contract.

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

Program Name	P.G. Diploma in Cyber Law	Program Code	
Course Name	IPR in Cyber World	Course Code	24LAWC102DS02
Credits	4	No. of hours/Week	4
Duration of End term examination	3 hours	Max. marks	100 Theory - 70 Marks (External) and 30 Marks (Internal)].

Note: The syllabus is divided in four units. The Examiner will set nine questions in all. First eight questions will be set by taking two questions from each unit. Question no. nine will consist of seven parts from all four units. The students have to attempt five questions in all selecting one question each from unit-I to IV. Question no. nine will be compulsory.

Learning Objectives:
1. Acquainting of 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 providing the concepts of Patent in Cyber world.

Learning Outcomes:
1. The studentswill be understands the scope of IPR issues in cyber world.
2. The studentswill be able to knows in detail about important national and international conventions.
3. The studentswill aware of the provisions relating to IPR in cyber world.
4. The studentswill have broad understanding of the application of IPR to Computer Technology
5. The students will be able to 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. Duggal, Pavan (2014) Legal Framework on Electronic Commerce and Intellectual Property Rights in Cyberspace, Universal Law Publishing - An imprint of Lexis Nexis
2. Elkin-Koren, Niva and Salzberger, Eli M. (2004) Law, Economics and Cyberspace: The Effects of Cyberspace on the Economic Analysis of Law (New Horizons in Law and Economics series),Edward Elgar Publishing Ltd
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
5. Unni, V.K. (2005) Trade Mark and the Emerging Concepts of Cyber Property Rights,Eastern Law House

Program Name	P.G. Diplomain Cyber Law	Program Code	
Course Name	Investigation of Cyber Crimes	Course Code	24LAWC102DS03
Credits	4	No. of hours/Week	4
Duration of End term examination	3 hours	Max. marks	100 Theory - 70 Marks (External) and 30 Marks (Internal)].

Note: The syllabus is divided in four units. The Examiner will set nine questions in all. First eight questions will be set by taking two questions from each unit. Question no. nine will consist of seven parts from all four units. The students have to attempt five questions in all selecting one question each from unit-I to IV. Question no. nine will be compulsory.

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

Learning Outcomes:
1. The student will have better knowledge of Cyber Crimes.
2. The students will have competence to understand the procedure of investigation of cyber crime.
3. The students will be ableto knows the power and functions of investigating agency.
4. The students will be able to knows the importance of digital evidence.
5. The student will have 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. Britz (2011) Computer Forensics and Cyber Crime: An Introduction,Pearson Education India
2. Marcella Jr., Albert (2007) Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Second Edition (Information Security), Auerbach Publications
3. Reyes, Anthony and Brittson, Richard (2007) Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors, Syngress
4. Reddy, Niranjan (2019) Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations, ApressStaniforth, Andrew and Akhgar, Babak (2017) Blackstone's Handbook of Cyber Crime Investigation.

Program Name	P.G. Diploma in Cyber Law	Program Code	
Course Name	E-Commerce and Taxation	Course Code	24LAWC102DS04
Credits	4	No. of hours/Week	4
Duration of End term examination	3 hours	Max. marks	100 Theory - 70 Marks (External) and 30 Marks (Internal)].

Note: The syllabus is divided in four units. The Examiner will set nine questions in all. First eight questions will be set by taking two questions from each unit. Question no. nine will consist of seven parts from all four units. The students have to attempt five questions in all selecting one question each from unit-I to IV. Question no. nine will be compulsory.

Course Objectives:
1. Students will be acquainted with privity of contract and jurisdiction issues in E-commerce
2. The students will learn about digital signature, security issues and UNCITRAL model law on E-commerce
3. Students will understand of issues relating to electronic money, credit cards and regulating transactions
4. Students will know about constitutional basis of tax and scope of total income
5. Students will have acquaintance with basic concepts of E-commerce transactions and legal issues pertaining to it

Learning Outcomes:
1. Students will become familiar with legal issue of jurisdiction in E-commerce
2. Students will get equipped with knowledge of digital signature and other security issues pertaining to technology in the cyber space.
3. Students will be able to identity issues pertaining to electronic money and their regulating transactions
4. Students will develop their understanding regarding constitutional basis of tax
5. Students will get theoretical knowledge and practical issues pertaining to E-commerce and taxation

Unit 1
1. Privity of Contracts
2. Jurisdiction issues in E-Commerce
3. Raising Capital for E Business

Unit 2
1. Digital Signatures
2. Security issues in E-Commerce
3. UNCITRAL model law of E-Commerce

Unit 3
1. Electronic Money
2. Regulating e-transactions
3. Role of RBI and Legal issues
4. Credit Card and Internet

Unit 4
1. Constitutional Basis of Tax
2. Residential status of assesse (company)
3. Scope of total income

REFERENCE READINGS:
1. Singh, Rav Pratap (2022), Constitution of Tax, OakBridge Publishing
2. Joseph, S.J. P.T. (2019), E-COMMERCE : AN INDIAN PERSPECTIVE, PHI Learning Pvt. Ltd
3. Ahuja and Astha (2022), E Commerce and Gst In India, New Century Publications
4. Jayan, S D (2011), Electronic Signature, CBS Publication
5. Jain Tarun(2018), Goods and Services Tax - Constitutional Law and Policy, Eastern Book Company

Program Name	P.G. Diploma in Cyber Law	Program Code	
Course Name	International Cyber Law	Course Code	24LAWC102DS05
Credits	4	No. of hours/Week	4
Duration of End term examination	3 hours	Max. marks	100 Theory - 70 Marks (External) and 30 Marks (Internal)

Note: The syllabus is divided in four units. The Examiner will set nine questions in all. First eight questions will be set by taking two questions from each unit. Question no. nine will consist of seven parts from all four units. The students have to attempt five questions in all selecting one question each from unit-I to IV. Question no. nine will be compulsory.

Course Objectives:
1. Students will be acquainted with UNCITRAL Model Law
2. Students will learn about WTO and TRIPS provisions related to cyber world
3. Students will understand of issues relating to cyber crime and their investigation by Interpol
4. Students will know about report on global cyber crimes and their effect on countries
5. Students will have acquaintance with basic international organizations dealing with cyber crimes.

Learning Outcomes:
1. Students will become familiar with European Union Convention on Cyber Crime
2. Students will get equipped with knowledge of uniform domain name dispute resolution policy
3. Students will be able to understand the web content accessibility guidelines
4. Students will develop their understanding role of ICC in cyber crimes
5. Students will get theoretical knowledge aboutworking of different International Organizations working to combat the cyber crimes

Unit 1
1. Electronic Data Interchange (EDI)- Concept and Legal Issues
2. UNCITRAL Model Law
3. European Union (EU) Convention on Cyber Crime

Unit 2
1. Internet Corporation for Assigned Names and Numbers (ICANN)
2. Uniform Domain Name Dispute Resolution Policy (URDP)
3. WTO & TRIPS

Unit 3
1. Interpol & Europol
2. Net Neutrality & EU Electronic Communication Regulatory Framework
3. Web Content Accessibility Guidelines (WCAG)

Unit 4
1. Global Cyber Crime Report, International Case Laws
2. Cyber Crime cases in international courts- International Criminal Court
3. Measures taken following the unprecedented cyber attack on ICC

REFERENCE READINGS:
1. https://www.icc-cpi.int/news/measures-taken-following-unprecedented-cyber-attack-icc
2. Sundram, Jae (2022), WTO Law and Policy, Routledge Publishing
3. Martha, Rutsel Silvestre J, et. all (2022),The Legal Foundations of Interpol, Hart Publishing
4. Siman, P. Rinas (2021), Telecommunications Liberalization to Net Neutrality Rules: A Longitudinal Institutional Analysis of EU Communications Policy, Springer
5. https://www.w3.org/TR/WCAG21/ & https://www.w3.org/WAI/standards-guidelines/wcag/
6. https://www.coe.int/en/web/cyberviolence/international-case-law

Program Name	P.G. Diploma in Cyber Law	Program Code	
Course Name	*Internship	Course Code	24LAWC102IN01
Credits	4	No. of hours/Week	3
Duration of End term examination	---	Max. marks	100 Marks (70 marks for Internship Report and 30 marks for presentation before committee)

Learning Objectives:
1. Acquainting to the students with practical aspects in the concerned field.
2. Providing to the students an opportunity to work with expert in the concerned field.
3. Providing the students a chance to develop clarity of law in practice.
4. To make the students to understand the working of the practitioners in the concerned field.
5. To make the students competent to deal with the issues and problems of the victims and help them with a professional approach.

Learning Outcomes:
1. The students will be able to knows about the concerned subject in practical sense.
2. The students will be more efficient in dealing with problems in the area.
3. The students will be able in builds up a professional approach in helping the victims/clients.
4. The students will be able to evolve in the relevant area with complete understanding of subjects.
5. The student will be more pro-active in expanding his legal and social understanding of the laws.

*The student has to undergo an internship for 3 weeks for Skill Enhancement with the organization/Firm/Unit, advocate in the concerned field. On completion of the internship, the student has to produce a certificate from such organization/Firm/Unit or advocate or expert person in the concerned field to the effect that he/she has completed the internship. The student has to prepare a detailed internship report which will carry 70 marks. The Viva-Voce Examination/Presentation of the report for 30 marks shall be conducted by a committee of three examiners consisting of HOD/his nominee, teacher concerned and one external examiner.