FACULTY OF LAW

ACADEMIC CURRICULA

POSTGRADUATE DEGREE PROGRAMME

Legum Magister (Cyber Law and Security)

(LLM)

TWO Years

Learning Outcome Based Education

Choice Based Flexible Credit System

Academic Year

2024 - 2025

FACULTY OF LAW

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Deemed to be University u/s 3 of UGC Act, 1956)

Kattankulathur, Chengalpattu District 603203, Tamil Nadu, India

// This page is intentionally left blank

1. Vision Statement	
Stmt - 1	*To attain a globally recognized position in the field of legal education, practice and research*
Stmt - 2	*To create a unique learning experience in legal education that are of international standards*
Stmt - 3	*To…..*

2. Mission Statement	
Stmt - 1	*To create, construct, disseminate knowledge and help learners to acquire professional skills and practices in the legal profession*
Stmt - 2	*To cultivate a research mindset and conduct research on facts, concepts, principles, theories and laws in legal education and legal practice*
Stmt - 3	*To produce law professionals who possess intellectual genius, moral consciousness, honor values, maintain integrity, honesty and social responsibility to ensure Rule of Law in the Constitution of India*
Stmt - 4	*To maintain the highest Quality standards in professional knowledge dissemination, research and in behavior*
Stmt - 5	*To….*

3. Program Education Objectives (PEO)	
PEO - 1	*To acquire and apply legal knowledge, practice skills to address the socio-legal challenges, constitutional legislative & societal transformation in society*
PEO - 2	*To acquire clinical skills in arguing, pleading, drafting, negotiating, conveyancing that are required for an ethical legal professional practice in Courts, Industries and other Corporates*
PEO - 3	*To develop legal research skills and legal reasoning, analysis and apply it during the Programme and in legal practice*
PEO - 4	*To provide a platform of self-employability and entrepreneurial skills by developing professional skills in legal industry*
PEO - 5	*To become skilled in legal research, written and oral communication, teamwork, advocacy, and problem-solving*

4. Consistency of PEO's with Mission of the Department

	Mission Stmt. - 1	Mission Stmt. - 2	Mission Stmt. - 3	Mission Stmt. - 4	Mission Stmt. - 5
PEO - 1	*H*	*H*	*H*	*M*	*M*
PEO - 2	*H*	*H*	*H*	*M*	*M*
PEO - 3	*H*	*H*	*H*	*M*	*M*
PEO - 4	*M*	*M*	*M*	*H*	*H*
PEO - 5	*M*	*M*	*M*	*H*	*H*

H – High Correlation, M – Medium Correlation, L – Low Correlation

5. Consistency of PEO's with Program Learning Outcomes (PLO)

	Program Learning Outcomes (PLO)											
	1. Disciplinary Knowledge	2. Critical Thinking	3. Problem Solving	4. Analytical Reasoning	5. Research-related Skills	6. Communication Skills	7. Cooperation/Team Work	8. Digital Literacy	9. Self-directed Learning	10. Moral and Ethical Reasoning	11. Leadership Qualities	12. Life Long Learning
PEO - 1	*H*	*H*	*M*	*H*	*H*	*H*	*M*	*H*	*M*	*H*	*H*	*H*
PEO - 2	*H*	*M*	*M*	*H*	*H*	*H*	*M*	*H*	*H*	*H*	*H*	*H*
PEO - 3	*M*	*M*	*M*	*H*	*H*	*H*	*M*	*M*	*M*	*H*	*M*	*H*
PEO - 4	*H*	*M*	*M*	*H*	*H*	*H*	*H*	*M*	*M*	*H*	*M*	*H*
PEO - 5	*H*	*H*	*M*	*H*	*H*	*H*	*M*	*M*	*H*	*H*	*H*	*H*

H – High Correlation, M – Medium Correlation, L – Low Correlation

6. Programme Structure(Total Credits : 90 Credits)

1. Professional Core Courses (C)

(11 Courses)

Course Code	Course Title	Hours/ Week L	T	P	C
PLCS24101T	*Law and Justice in the Globalizing World*	*3*	*1*	*2*	*5*
PLCS24102T	*Comparative Public Law*	*3*	*1*	*2*	*5*
PLCS24103T	*Fundamentals of Computer Science and Cyber security*	*3*	*1*	*2*	*5*
PLCS24104T	*Introduction to Cyberspace, Cyber Law and Security*	*3*	*1*	*2*	*5*
PLCS24201T	Judicial Process	*3*	*1*	*2*	*5*
PLCS24202T	*Cybercrimes and Cybersecurity*	*3*	*1*	*2*	*5*
PLCS24203T	*Constitutional and Legal aspects of Cyberspace and Internet*	*3*	*1*	*2*	*5*
PLCS24204T	*International and National Perspective of Cyber Law*	*3*	*1*	*2*	*5*
PLCS24301T	*Legal Research Methodology*	*3*	*1*	*2*	*5*
PLCS24302T	*Cyber Forensics and Evidential Issues*	*3*	*1*	*2*	*5*
PLCS24303T	*Procedural Issues of Cyber Law*	*3*	*1*	*2*	*5*
Total Learning Credits					55

2. Professional Elective Courses (E)

(4 Courses)

Course Code	Course Title	Hours/ Week L	T	P	C
PLCS24304T	*National Defense, Telecommunication and Cybersecurity*	*3*	*1*	*2*	*5*
PLCS24305T	*Intellectual Property Rights and Cybersecurity*	*3*	*1*	*2*	*5*
PLCS24401T	*Cryptocurrency and Legal issues*	*3*	*1*	*2*	*5*
PLCS244402T	*Artificial intelligence and Cybersecurity*	*3*	*1*	*2*	*5*
Total Learning Credits					20

4. Clinical Courses(L)

(6 Courses)

Course Code	Course Title	Hours/ Week L	T	P	C
PLCS24306P	*Mini Project*	*0*	*1*	*4*	*3*
PLCS24403P	*Dissertation*	*0*	*2*	*20*	*12*
Total Learning Credits					15

1. Implementation Plan

SEMESTER - I

Code	Course Title	Hours/ Week			C
		L	T	P	
PLCS24101T	Law and Justice in the Globalising World	3	1	2	5
PLCS24102T	Comparative Public Law	3	1	2	5
PLCS24103T	Fundamentals of Computer Science and Cyber security	3	1	2	5
PLCS24104T	Introduction to Cyberspace, Cyber Law and Security	3	1	2	5
	Total Learning Credits				**20**

SEMESTER - II

Code	Course Title	Hours/ Week			C
		L	T	P	
PLCS24201T	Judicial Process	3	1	2	5
PLCS24202T	Cybercrimes and Cybersecurity	3	1	2	5
PLCS24203T	Constitutional and Legal aspects of Cyberspace and Internet	3	1	2	5
PLCS24204T	International and National Perspective of Cyber Law	3	1	2	5
	Total Learning Credits				**20**

SEMESTER - III

Code	Course Title	Hours/ Week			C
		L	T	P	
PLCS24301T	Legal Research Methodology	3	1	2	5
PLCS24302T	Cyber Forensics and Evidential Issues	3	1	2	5
PLCS24303T	Procedural Issues of Cyber Law	3	1	2	5
PLCS24304T	National Defense, Telecommunication and Cybersecurity	3	1	2	5
PLCS24305T	Intellectual Property Rights and Cybersecurity	3	1	2	5
PLCS24306P	Mini Project	0	1	4	3
	Total Learning Credits				**28**

SEMESTER - IV

Code	Course Title	Hours/ Week			C
		L	T	P	
PLCS24401T	Cryptocurrency and Legal issues	3	1	2	5
PLCS24402T	Artificial intelligence and Cybersecurity	3	1	2	5
PLCS24403D	Dissertation	0	2	20	12
	Total Learning Credits				**22**

Total No. Learning Credits : 90

2. Program Articulation Matrix

Course Code	Course Name	Programme Learning Outcomes											
		Disciplinary Knowledge	Critical Thinking	Problem Solving	Analytical Reasoning	Research-related Skills	Communication Skills	Cooperation/Team Work	Digital Literacy	Self-directed Learning	Moral and Ethical Reasoning	Leadership Qualities	Life Long Learning
PLCS24101T	Law and Justice in the Globalizing World	3	2	2	3	2	3	-	2	2	3	3	1
PLCS24102T	Comparative Public Law	3	2	2	3	2	3	1	2	2	2	3	1
PLCS24103T	Fundamentals of Computer Science and Cybersecurity	3	2	1	2	2	3	1	2	2	2	3	2
PLCS24104T	Introduction to Cyberspace, Cyber Law and Security	3	3	1	2	2	3	-	2	2	2	3	1
PLCS24201T	Judicial Process	3	2	2	3	2	3	-	2	2	2	3	2
PLCS24202T	Cybercrimes and Cybersecurity	3	3	2	2	2	3	1	2	2	3	3	2
PLCS24203T	Constitutional and Legal aspects of Cyberspace and Internet	3	2	3	3	2	3	-	2	2	3	3	2
PLCS24204T	International and National Perspective of Cyber Law	3	3	3	3	2	3	1	2	2	2	3	3
PLCS234301T	Legal Research Methodology	3	2	2	3	2	3	-	2	2		3	2
PLCS24302T	Cyber Forensics and Evidential Issues	3	2	2	3	2	3	-	2	2	2	3	1
PLCS24303T	Procedural Issues of Cyber Law	3	2	2	3	2	3	1	2	2	3	3	1
PLCS24304T	National Defense, Telecommunication and Cybersecurity	3	2	2	3	2	3	1	2	3	3	2	-
PLCS24305T	Intellectual Property Rights and Cybersecurity	3	2	2	3	2	3	1	2	3	2	2	-
PLCS24306P	Mini Project	-	1	2	-	3	1	-	3	3	3	2	-
PLCS24401T	Cryptocurrency and Legal issues	3	2	2	3	2	3	-	2	2	3	3	1
PLCS24402T	Artificial intelligence and Cybersecurity	3	2	2	3	2	3	1	2	2	3	3	-
PLCS24403P	Dissertation	-	2	2	-	3	1	1	3	3	3	2	2

H – High Correlation, M – Medium Correlation, L – Low Correlation

Code	PLCS24101T	Title	LAW AND JUSTICE IN GLOBALISING WORLD	Category		Professional Core	L	T	P	C
							3	1	2	5

Course Offering Department	School of Law	Pre-requisite Courses	NIll	Co-requisite Courses	Nill	Progressive Courses	Nill	Data Book / Codes/Standards	

Title & Content	INTRODUCTION	GLOBALIZATION AND FREE MARKET	CONCEPT OF JUSTICE IN GLOBALISING WORLD	GLOBALIZATION AND CULTURAL IMPACT	GLOBALIZATION AND CONFLICT RESOLUTION
Duration (hour)	18	18	18	18	18
SLO-1	*Examine what globalization means. And An outline of globalization's history The forces behind globalization Explore about the scope and significance of globalization*	*Examine the concept of globalization and free market, Elucidate the historical context of globalization and its relationship with free market principles*	*Analyze the difficulties and intricacies of attaining justice in a worldwide world, the influence of universal values on creating ideas of justice, and how justice is changing in response to globalization.*	*Comprehend the concept of globalization and its influence on culture.*	*Identify the foundational concepts of globalization and its impact on conflicts worldwide*
SLO-2	*Examine how globalization has affected culture. Identity and globalization Inequalities in society within a globalized world* *Case studies illustrating globalization's effects on society*	*Extrapolate the fundamental principles and characteristics of free market economics Analyze the impact of globalization on the expansion of free market ideologies*	*Examine The tension between cultural relativism and universalism in the context of justice.*	*Examine the tensions between cultural homogenization and cultural diversity in a globalizing world.*	*Analyze the causes and characteristics of international conflicts in a globalized world*
SLO-3	*examine International governance frameworks The mechanics of power in a worldwide society Subnational government versus national sovereignty Case studies of globalization's political effects.*	*Analyze possible approaches for preserving or modifying the welfare state in response to globalization.*	*Analyze The concepts of fairness, equality, and solidarity within the framework of global justice, and the difficulties associated with implementing principles of justice across international boundaries.*	*Gain a comprehensive understanding of the impact of globalization on cultural heritage places, traditions, and behaviors.*	*Explore the role of diplomatic negotiations, mediation, and arbitration in resolving disputes*
SLO-4	*Tutorial:Comparative analysis of trade and globalization, focusing on foreign direct investment (FDI) and multinational corporations (MNCs)..*	*Tutorial: Discuss comprehensive understanding of different methods to balance welfare state ,free market and global economy*	*Tutorial: Engage in an in-depth discussion on principles of justice and equity and its evolution in the modern times*	*Tutorial: Analyze the international laws and principles in preserving culture*	*Tutorial: Examine the legal frameworks governing , exploring key treaties, agreements, and legal principles.*

SLO-5	*Practice: Analyze case studies in different countries post globalization*	*Practice: Examine methods to address legal issues in free market*	*Practice: Examine the methods of handling crisis in global justice*	*Practice: Evaluate the cases in which globalization deteriorated culture and revitalization measures*	*Practice: Analyze strategies for addressing grievances, promoting reconciliation, and building inclusive societies*
SLO-6	*Practice: Engage in discussion on landmark cases illustrating the interpretation and application of laws in globalized world order*	*Practice: Explore special provisions related to international trade laws and other legislations to secure a global welfare state*	*Practice: Explore the various methods to in which universal principles influenced laws in nations*	*Practice: case studies on cultural appropriation and its impact on cultural heritage preservation*	*Practice: Examine and compare different strategies for promoting media literacy and constructive dialogue to support conflict resolution efforts*
SLO-7	*elucidate the meaning and application of international law.* *Transnational legal framework examples* *Opportunities and challenges associated with global law*	*Examine the utilization and administration of natural resources in a worldwide economy.*	*Gain an understanding of The ethical responsibilities of individuals and societies within a cosmopolitan perspective, as well as the conflicts that arise between cosmopolitan principles and national interests.*	*Examine the influence of Western hegemony in the global media on cultural diversity.*	*Examine the legal frameworks governing international taxation, focusing on bilateral and multilateral agreements that shape cross-border taxation policies.*
SLO-8	*Discuss the idea of state sovereignty,Globalization and sovereignty: issues for national security in a globalized world*	*Examine the socioeconomic consequences of relocation resulting from development projects.,the ethical factors associated with the displacement of people for the purpose of development. and alternate strategies for development that give priority to social justice and human rights.*	*examine impact of globalization on the judicial process and legal systems and challenges of regulating transnational activities and enforcing global justice*	*Examine the impact of migration and transnationalism on cultural identities and behaviors.*	*Explore the role of media in exacerbating and mitigate conflicts through framing, propaganda, and peace journalism*
SLO-9	*Analyze the notions of Federalism and Globalization Decentralization and globalization Globalization's effects on democratic processes*	*Evaluate potential policy interventions to reduce economic inequality and promote social cohesion*	*Gain an understanding on diverse perspectives and arguments on issues such as economic inequality, human rights abuses, and environmental degradation*	*Analyze How globalization affects indigenous peoples' rights, languages, and cultural practices*	*Analyze the contributions of organizations such as the United Nations, NATO, and regional bodies to global peacekeeping efforts*
SLO-10	*Tutorial: Conduct in-depth discussions on fundamental principles of transnational laws and their applications.*	*Tutorial: discuss the social welfare laws intended to prevent social and economic disparity caused by globalization*	*Tutorial: Discuss the international judicial process*	*Tutorial – Discuss the power dynamics involved in cultural resistance and negotiation in a globalized world*	*Tutorial –Discuss the role of peacekeeping missions and interventions in resolving international conflicts*

SLO-11	*Practice: Conduct a workshop on essential concepts and provisions related to transnational laws and its binding effects*	*Practice: explore the ways in which globalization and free market policies contribute to economic inequality.*	*Practice: Explore the ways in which one nations act can impact another nation and the recourse available*	*Practice: Analyze case studies to assess the impact of globalization in indigenous community*	*Practice: Analyze double taxation scenarios, applying the principles of Double Taxation Avoidance Agreements (DTAA) to resolve issues and ensure fair tax treatment.*
SLO-12	*Practice: Explain and discuss essential laws that serves as foundation for globalization*	*Practice: Analyze case studies involving loss of livelihood due to development and alternate measures taken .*	*Practice:Explore case studies on cross-border legal disputes and their implications for the administration of justice*	*Practice: Engage in developing various legal approaches to preserve indigenous culture and traditional knowledge and practices .*	*Practice: case studies illustrating successful and unsuccessful peacekeeping efforts*
SLO-13	*Explain international trade law frameworks Discuss dispute resolution mechanisms in trade law Analyze the impact of globalization on trade liberalization*	*Examine the rise of consumer culture in a globalized society and analyze the influence of consumerism on individual conduct and societal principles.*	*Acquire knowledge related to the role of international human rights law and institutions in promoting global justice*	*Comprehend the strategies for promoting gender equality and cultural diversity in a globalized society*	*.Analyze the importance of multilateralism in addressing global conflicts*
SLO-14	*Analyze the impact of legislative changes on individuals and businesses.*	*Examine the influence of free market principles on cultural trends and practices, emphasize the significance of safeguarding cultural diversity in an interconnected society, and explore methods for fostering cultural plurality and facilitating intercultural interaction.*	*Gain an understanding of The concept of environmental justice within the framework of globalization.*	*Comprehend the challenges of cultural governance in balancing economic, social, and cultural priorities*	*Analyze how climate change exacerbates existing conflicts and contributes to new security challenges*
SLO-15	*comprehend the main ideas that have been discussed thus far.Talk about recent occurrences pertaining to globalization.Examine how globalization has affected current concerns.*	*Comprehend role of civil society and grassroots movements in advocating for global regulation Elucidate the tensions between national sovereignty and global governance in a free market economy.*	*Comprehend the The obstacles encountered by women and individuals who identify as gender minorities in obtaining legal recourse on a global scale.*	*examine the concept of soft power and its influence on global cultural dynamics*	*Examine the impact of technology on conflict dynamics, including cyber warfare, surveillance, and information warfare*
SLO-16	*Tutorial: Provide an overview of international legislation in the era of globalization*	*Tutorial: Explain case scenarios and simulate issues related to tensions between sovereigns and diplomatic ideals*	*Tutorial: Analyze case scenarios involving global justice .*	*Tutorial: Gain an understanding of the practical insights into the ethical considerations and challenges of cultural diplomacy in a globalized world*	*Tutorial: Analyze contemporary challenges in international regulations through real-world case studies, exploring solutions and best practices.*

SLO-17	*Practice: Evaluate participants' ability to navigate complexities in determining cases involving multiple sovereigns*	*Practice: Evaluate case studies to identify legal solutions for conflicts between sovereigns*	*Practice: Engage in debates and critical discussions on controversial global justice topics*	*Practice: emerging trends and debates in the field of cultural globalization*	*Practice: Identify the importance of sustained engagement and advocacy for promoting global peace and security*
SLO-18	*Practice: Enhance participants' critical thinking and problem-solving skills in addressing complex transnational issues*	*Practice: Assign and analyze case studies involving problems that require multinational intervention*	*Practice: Examine penalties and offenses of states that impacts another*	*Practice: Analyze case studies presenting real-world best practices and innovative approaches to cultural-legal policy and management*	*Practice: Engage in discussion on scenario analysis, and presentations on future trends in global conflicts*

Resources			
1	Andrew Kuper, Democracy Beyond Borders: Justice and Representations in Global Institutions (OUP, 2006).	2	David B. Goldman, Globalization and the Western Legal Tradition: Recurring Patterns of Law and Authority (Cambridge University Press, 2008).
3	Anthony McGrew, David Held (eds), Governing Globalization: Power, Authority and Global Governance (Polity Press, 2002).	4	World Commission on Social Dimension of Globalization, A Fair Globalization: Creating Opportunities for All (2004).
5	Simon Coney, Justice Beyond Borders: A Global Political Theory (Oxford University Press, 2005).		

Rationale (CLR)	*The purpose of learning this course is to:*	Depth				Attainment			Program Learning Outcomes (PLO)											
		1	2	3	4	1	2	3	1	2	3	4	5	6	7	8	9	10	11	12
CLR-1	*Acquire a foundational understanding of laws in the era of globalization including background of transnational law applicability of set legal principle across sovereigns*																			
CLR-2	*Equip participants with advanced knowledge and practical skills in dealing with legal issues across borders*																			
CLR-3	*Provide participants with a comprehensive understanding of distributive justice and international judicial process*																			
CLR-4	*Equip participants with comprehensive knowledge and practical proficiency in Preservation of Cultural Heritage in a Globalized Environment*																			
CLR-5	*Equip participants with advanced proficiency in Global Diplomacy and Multilateral Approaches to Conflict Resolution*																			

Outcomes (CLO)	*At the end of this course, Students will be able to:*	*Conceive*	*Design*	*Implement*	*Operate*	*Level of Thinking*	*Expected Proficiency (%)*	*Expected Attainment (%)*	*Disciplinary Knowledge*	*Critical Thinking*	*Problem Solving*	*Analytical Reasoning*	*Research-related Skills*	*Communication Skills*	*Cooperation/Team Work*	*Digital Literacy*	*Self-directed Learning*	*Moral and Ethical Reasoning*	*Leadership Qualities*	*Life Long Learning*
CLO-1	*Develop a profound understanding of the fundamentals of law in the globalized world, including the origins of transnational law and the applicability of a given legal theory across sovereigns.*	□	□		-	*2*	*85*	*75*	*3*	-	-	*1*	-	*3*	-	*2*	*2*	*1*	*2*	*3*
CLO-2	*Master complex issues involving jurisdictional questions on critical areas such as environmental impacts and natural resources across border*	□	□	□	-	*2*	*85*	*75*	*3*	*2*	*1*	*2*	*2*	*3*	-	*1*	*2*	*1*	*2*	*3*
CLO-3	*Analyze transnational issues involving global distributive justice and acquire remedies via international judicial process*	□	□	□	✓	*3*	*85*	*75*	*3*	*1*	*3*	*1*	*3*	*3*	-	*1*	*1*	*2*	*1*	*3*
CLO-4	*Acquire comprehensive legal knowledge in Preservation of Cultural Heritage,cultural identity and language in a Globalized Environment*	□	□	□	□	*3*	*85*	*75*	*3*	*3*	*2*	*3*	*3*	*3*	-	*2*	*3*	*3*	*3*	*3*
CLO-5	*Apply international principles in Multilateral Approaches to Conflict Resolution*	□	□	□	□	*3*	*85*	*75*	*3*	*3*	*2*	*3*	*3*	*3*	-	*3*	*3*	*3*	*3*	*3*

Assessment Method (Max. Marks: 100)

Level of Thinking		Continuous Learning Assessment (CLA 40% Weightage)								Final Exam	
		Model Exam (20%)		Assignment/ Seminar/Group discussion/ Presentation (10%)		Participation in seminar/ Conference/ Publication (5%)		Participation in class room/co-curricular & Para curricular activities (5%)		(60%)	
1	Remember	40%	-	40%	-	30%	-		-	40%	-
2	Understand										
3	Apply	40%	-	40%	-	40%	-		-	40%	-
4	Analyze										
5	Evaluate	20%	-	20%	-	30%	-		-	20%	-
6	Create										
Total		100 %		100 %		100 %		100 %		100 %	

Strategies					
Simulations	☐	Clarification/Pauses	☐	Quality Education	☐
Presentation Tools				Good health and well- being	☐
Learning Management System		Group Discussion	☐	Reduced Inequalities	☐
		Group task	☐		
		Debate	☐		
		Interactive Lecture	☐		
		Case studies	☐		

Designers					
Professional Experts		Higher Institution Experts		Internal Experts	
1	*Dr. Manoj Mate, Associate Professor of Law, DePaul University College of Law*	*1*	*Dr. Ayan Hazra, Assistant Professor, HNLU*	*1*	*Prof. (Dr.)Sree Sudha, Dean , School of Law, SRM IST*
2		2		2	

Code	PLCS24102T	Title	COMPARATIVE PUBLIC LAW	Category		Professional Core	L	T	P	C
							3	1	2	5

Course Offering Department	School of Law	Pre-requisite Courses		Co-requisite Courses		Progressive Courses		Data Book / Codes/Standards	

Title & Content	COMPARATIVE CONSTITUTIONAL LAW	CONSTITUTIONAL FOUNDATIONS OF POWERS	SOVEREIGNTY: THEORY OF CONSTITUTIONAL STATE	CONSTITUTIONAL REVIEW	EMERGING TRENDS IN COMPARATIVE PUBLIC LAW
Duration (hour)	18	18	18	18	18
SLO-1	*Analyze the role of constitutions as supreme laws in various legal system*	*Examine the significance of constitutional foundations in shaping governmental powers*	*Analyze sovereignty and its importance in political theory*	*Comprehend the Definition and significance of constitutional review*	*introduction to emerging topics in the field*
SLO-2	*Examine Historical development of constitutionalism*	*Extrapolate the powers and functions of the legislature in lawmaking*	*Examine role of the sovereign in safeguarding individual rights and freedoms*	*Examine different methods such as judicial, political, and concentrated review*	*Analysis of challenges to constitutionalism globally*
SLO-3	*Examine the principles underlying constitutional design, such as separation of powers, checks and balances, and rule of law.*	*Analyze the significance of the rule of law in ensuring government accountability and protecting individual rights*	*Analyze The principles of legislative supremacy and the rule of law within the constitutional state framework*	*Gain a comprehensive understanding of the i role of courts in interpreting and applying constitutional provisions*	*Explore the threats to the rule of law and democratic institutions*
SLO-4	*Tutorial:Comparative analysis of constitution in various nations*	*Tutorial: Discuss comprehensive understanding of different methods to ensure constitutional supremacy*	*Tutorial: Engage in an in-depth discussion on principles of constitutional principles and equity and its evolution in the modern times*	*Tutorial: Analyze the iImportance of constitutional review in upholding the rule of law*	*Tutorial: Discussion on the relevance and implications of studying emerging topics*
SLO-5	*Practice: Analyze case studies in different countries related to constitutional cases*	*Practice: Examine methods to address legal issues in constitution*	*Practice: Examine the methods of handling constitutional crisis*	*Practice: Evaluate the cases in which constitutional review aided in preservation of constitution*	*Practice: Discussion on issues such as digital rights, privacy, and surveillance*
SLO-6	*Practice: Engage in discussion on landmark cases illustrating the interpretation and application of constitutional provisions in different nations*	*Practice: Explore special provisions related to rule of law and separation of power*	*Practice: Explore the various methods to in which universal principles influenced constitutional laws in nations*	*Practice: case studies on landmark constitutional reviews*	*Practice: Examine and compare different methods to handle violation of constitutional rights by one sovereign's subjects by another*

SLO-7	*elucidate the role of comparative constitutional law in promoting constitutionalism, democracy, and human rights globally*	*Modern interpretations and extensions of the rule of law concept*	*Compare and contrast the constitutional state with the social state*	*Examine the influence of Western philosophies in the constitutional review mechanism*	*Examine environmental rights and justice in constitutional contexts*
SLO-8	*Discuss the challenges and limitations of comparative constitutional*	*Examine the the inclusion of social and economic rights within the rule of law framework*	*examine theories of natural rights, social contract, and human dignity in grounding constitutional rights*	*Examine the political dynamics and implications of political review processes*	*Analysis of post-conflict constitution-building processes*
SLO-9	*Analyze how constitutional design influences the distribution of power and decision-making processes*	*Evaluate the role of independent institutions, such as constitutional courts and auditing bodies, in maintaining checks and balances*	*Gain an understanding on the impact of globalization, neoliberalism, and welfare states on constitutional rights*	*Analyze concentrated review, focusing on specialized constitutional review bodies or courts*	*Analyze the contributions of organizations such as the United Nations, NATO, and regional bodies in preserving constitutions of countries*
SLO-10	*Tutorial: Conduct in-depth discussions on approaches to protecting fundamental rights in different constitutional systems*	*Tutorial: discuss the social welfare laws intended to enhance the principles of constitution*	*Tutorial: Discuss the constitutional rights litigation and social reform movements*	*Tutorial – Discuss the power dynamics involved in political review*	*Tutorial –Discuss the role of peacekeeping missions and interventions in preventing failure of constitution*
SLO-11	*Practice: Conduct a workshop on essential concepts and provisions related to universal constitutional provisions and its binding effects*	*Practice: case studies on the effectiveness of checks and balances in preventing governmental abuse of power*	*Practice: Explore the ways in which one nations act can impact another nation and the recourse available*	*Practice: Analyze case studies involving political review of constitution*	*Practice: Analyze regulatory responses to technological advancements*
SLO-12	*Practice: case studies on significant constitutional amendments and their implications*	*Practice:case studies on the enforcement of social and economic rights in different legal systems*	*Practice:Explore case studies on legislative reforms and constitutional amendments*	*Practice: Engage in developing various legal approaches to preserve constitution and its ideals*	*Practice:enumerate potential threats technology pose to constitutional values*
SLO-13	*Compare approaches to federalism and decentralization in different constitutional systems*	*Examine the rise of tyrannic governments and how constitutional provisions battling it*	*Acquire knowledge related to application of constitutional rights in addressing social and economic inequalities*	*Comprehend diffused review mechanisms, such as inter-branch checks and balances*	*.Analyze legal responses to climate change at national and international levels*

SLO-14	*Analyze the powers and limitations of constitutional courts in different legal systems*	*Examine the mechanisms for legislative oversight, such as committee hearings, inquiries, and budgetary control*	*Gain an understanding of strategies for defending sovereignty and constitutionalism in the face of challenges*	*Comprehend the limitations imposed on judicial review, such as justiciability, standing, and political questions*	*Analyze how climate change exacerbates existing issues and contributes to new constitutional challenges*
SLO-15	*comprehend the main ideas that have been discussed thus far.* *Talk about recent occurrences pertaining to globalization.* *Examine how globalization has affected current concerns.*	*Comprehend the challenges of ensuring judicial independence in practice, including political interference and corruption* *.*	*Compare different approaches to sovereignty and constitutionalism in diverse legal systems*	*examine the methodologies such as textualism, originalism, purposivism, and living constitutionalism*	*Examine the impact of technology on constitutionalism*
SLO-16	*Tutorial: Discuss case studies on landmark judicial review decisions and their impact on legal and political developments*	*Tutorial: Explain case scenarios and simulate issues related to constitutional violations*	*Tutorial: Analyze case scenarios involving constitutional violations*	*Tutorial: Gain an understanding of the practical insights into the ethical considerations and challenges in constitutional review*	*Tutorial: Analyze contemporary challenges to constitutions that are transitioning in to future challenges*
SLO-17	*Practice: case studies on successful and failed constitutional transitions*	*Practice: Evaluate case studies to identify legal solutions for deterioration of constitutional values*	*Practice: Engage in debates and critical discussions on global constitutional values*	*Practice: landmark judicial review cases from various jurisdictions*	*Practice: Identify the importance of sustained engagement and advocacy for promoting constitutionalism*
SLO-18	*Practice: Enhance participants' critical thinking and problem-solving skills in addressing complex constitutional l issues*	*Practice: Assign and analyze case studies involving problems on on judicial activism, judicial restraint*	*Practice: Examine future challenges to constitutionalism and values*	*Practice: Analyze key principles and doctrines developed through case laws*	*Practice: Engage in discussion on scenario analysis, and presentations on future trends in constitutionalism*

Resources			
1	D.D. Basu, Comparative Constitutional Law (Wadhwa and Company, 2008).	2	Dr.Subhash C Kashyap, Framing of Indian Constitution (Universal Law, 2004)
3	Mahendra P. Singh, Comparative Constitutional Law (Eastern Book Company, 1989).	4	Sunil Khilnani,VikramRaghavan, ArunThiruvengadam, Comparative Constitutionalism in South Asia (Oxford University Press, 2013).
5	M.V. Pylee, Constitution of the World (Universal, 2006)		

Rationale (CLR)	*The purpose of learning this course is to:*	Depth				Attainment			Program Learning Outcomes (PLO)											
		1	2	3	4	1	2	3	1	2	3	4	5	6	7	8	9	10	11	12
CLR-1	*Gain a comprehensive understanding of the fundamental principles of constitutional law, including separation of powers, federalism, checks and balances, and individual rights.*																			
CLR-2	*Equip students with a comprehensive understanding of constitutional principles and structures governing the distribution of powers within governmental systems, fostering critical analysis and ethical engagement with issues of governance and rights.*																			
CLR-3	*Elucidate the theory and practice of sovereignty within the framework of constitutional governance, examining its implications for the rule of law, individual rights, and democratic accountability.*																			
CLR-4	*Equip participants with comprehensive knowledge and practical proficiency in various methods of constitutional reviews and their limitations*																			
CLR-5	*Equip participants with advanced knowledge to prognosticate future constitutional challenges*																			
		Conceive	*Design*	*Implement*	*Operate*	*Level of Thinking*	*Expected Proficiency (%)*	*Expected Attainment (%)*	*Disciplinary Knowledge*	*Critical Thinking*	*Problem Solving*	*Analytical Reasoning*	*Research-related Skills*	*Communication Skills*	*Cooperation/Team Work*	*Digital Literacy*	*Self-directed Learning*	*Moral and Ethical Reasoning*	*Leadership Qualities*	*Life Long Learning*
Outcomes (CLO)	*At the end of this course, Students will be able to:*																			
CLO-1	*Comprehend the basic tenets of constitutional law, such as individual rights, federalism, checks and balances, and the division of powers.*	□	□		-	*2*	*85*	*75*	*3*	*-*	*-*	*1*	*-*	*3*	*-*	*2*	*2*	*1*	*2*	*3*
CLO-2	*Develop a profound understanding of the structural and constitutional precepts that regulate the allocation of authority within political institutions, encouraging moral and critical thinking on matters of rights and governance.*	□	□	□	-	*2*	*85*	*75*	*3*	*2*	*1*	*2*	*2*	*3*	*-*	*1*	*2*	*1*	*2*	*3*
CLO-3	*Analyze the concept and application of sovereignty in the context of constitutional governance, considering the effects it has on the rule of law, individual liberties, and democratic responsibility.*	□	□	□	□	*3*	*85*	*75*	*3*	*1*	*3*	*1*	*3*	*3*	*2*	*1*	*1*	*2*	*1*	*3*
CLO-4	*Acquire comprehensive legal knowledge on constitutional review,its purpose and methods*	□	□	□	□	*3*	*85*	*75*	*3*	*3*	*2*	*3*	*3*	*2*	*1*	*2*	*3*	*3*	*3*	*3*
CLO-5	*Apply constitutional principles and methods to preserve it against future challenges*	□	□	□	□	*3*	*85*	*75*	*3*	*3*	*2*	*3*	*3*	*3*	*-*	*3*	*3*	*3*	*3*	*3*

Assessment Method (Max. Marks: 100)

Level of Thinking		Continuous Learning Assessment (CLA 40% Weightage)								Final Exam	
		Model Exam (20%)		Assignment/ Seminar/Group discussion/ Presentation		Participation in seminar/ Conference/ Publication		Participation in class room/co-curricular & Para curricular activities			
		(20%)		(10%)		(5%)		(5%)		(60%)	
1	Remember	40%	-	40%	-	30%	-		-	40%	-
2	Understand										
3	Apply	40%	-	40%	-	40%	-		-	40%	-
4	Analyze										
5	Evaluate	20%	-	20%	-	30%	-		-	20%	-
6	Create										
Total		100 %		100 %		100 %		100 %		100 %	

Technology		Pedagogy / Andragogy		Sustainable Development	
Simulations		Clarification/Pauses		Quality Education	
Presentation Tools					
Learning Management System		Group Discussion		Reduced Inequalities	
		Group task			
		Debate			
		Interactive Lecture			
		Case studies			

Designers					
Professional Experts		Higher Institution Experts		Internal Experts	
1	*Dr. Madhav Khosla, Visiting Professor, Yale Law School*	1	*Dr.Aparna Chandra, Assistant Professor, National Law University, Delhi*	1	*Dr.Sreelatha I,Associate Professor, School of Law, SRMIST*
2	*Dr. Arghya Sengupta, Associate Professor, O.P. Jindal Global University*	2	*Dr S K Bose, Associate Professor,School of Law, Manav Rachna University*	2	

Code	PLCS24103T	Title	FUNDAMENTALS OF COMPUTER SCIENCE AND CYBER SECURITY	Category		Professional Core	L	T	P	C
							3	1	2	5

Course Offering Department	School of Law	Pre-requisite Courses	Fundamentals of computer	Co-requisite Courses	Nill	Progressive Courses	Nill	Data Book / Codes/Standards	

Title & Content	COMPARATIVE CONSTITUTIONAL LAW	CONSTITUTIONAL FOUNDATIONS OF POWERS	SOVEREIGNTY: THEORY OF CONSTITUTIONAL STATE	CONSTITUTIONAL REVIEW	EMERGING TRENDS IN COMPARATIVE PUBLIC LAW
Duration (hour)	18	18	18	18	18
SLO-1	*Students will analyze the legal implications of machine instructions and addressing modes, considering issues such as intellectual property and regulatory compliance.*	*Analyze the Entity-Relationship (ER) model, relational model, and their interconnections in database design.*	*Analyze the functionalities of TCP, UDP, and sockets, and their roles in facilitating communication between networked devices.*	*Examine the concept of cyberspace, elucidating its definition, architecture, and implications for modern communication technologies.*	*Analyze the components and intricacies of e-commerce, including its definition, main components, and security elements.*
SLO-2	*Students will understand the legal aspects related to ALU, data-path, and control unit, addressing issues such as liability and compliance.*	*Evaluate relational algebra, tuple calculus, and SQL as query languages, understanding their syntax, semantics, and application in database operations.*	*Evaluate congestion control mechanisms used in TCP/IP networks, understanding their importance in maintaining network stability and performance*	*Analyze the fundamental principles of computer and web technology, discerning their role in shaping cyberspace.*	*Examine the various threats posed to e-commerce platforms and evaluate security best practices to mitigate these risks.*
SLO-3	*Learners will explore legal considerations in the implementation of instruction pipelining, focusing on regulatory compliance and potential legal challenges.*	*Assess integrity constraints and normalization techniques, identifying dependencies and eliminating redundancy in database schemas.*	*Examine application layer protocols including DNS, SMTP, POP, FTP, and HTTP, and their respective roles in network communication and data exchange.*	*Explore communication and web technologies, unraveling their evolution, functionalities, and impact on cyberspace architecture.*	*Explore the concept of digital devices security, covering endpoint devices, mobile phones, and associated security measures.*
SLO-4	Tutorial: *Conducting a legal analysis of a hypothetical cyber security scenario involving ALU, data-path, and control unit components.*	*Tutorial – Design an ER model for a given dataset, identifying entities, relationships, and attributes.*	*Tutorial –Conduct an analyses t explore TCP/IP fundamentals, including TCP, UDP, and sockets, through interactive demonstrations and hands-on exercises.*	*Tutorial – Explore case studies of successful social media marketing campaigns, focusing on their effectiveness in enhancing customer engagement.*	*Tutorial – Identify through discussion that elements of e-commerce security and common threats and Discuss best practices for securing e-commerce platforms.*
SLO-5	*Practice: Reviewing and discussing landmark cases and analyzing legal cases related to technology and intellectual property*	*Practice : Engage in a workshop to design ER models for various real-world scenarios, emphasizing entity identification, relationship definition, and normalization.*	*Practice: Implement TCP and UDP socket communication in a simulated network environment.*	*Practice : Collaborate in groups to create diagrams and presentations illustrating the structure and functionality of cyberspace.*	*Practice: Respond to simulated security incidents, applying best practices to mitigate risks and protect sensitive information.*

SLO-6	*Practice: Drafting sample policies on data protection, cybersecurity, and ethical use of technology*	***Practice:** Practice writing SQL queries in a laboratory setting, covering basic to advanced operations, such as joins, subqueries, and aggregation functions.*	***Practice:** Configure and test various application layer protocols, including DNS, SMTP, POP, FTP, and HTTP.*	***Practice:** Engage in hands-on exploration of various social media platforms to understand their functionalities and usage scenarios.*	***Practice:** Configure security settings on various digital devices, including endpoint devices and mobile phones.*
SLO-7	*Students will examine the legal implications surrounding memory hierarchy, including cache, main memory, and secondary storage, addressing privacy and data protection concerns.*	*Examine file organization and indexing methods, such as B and B+ trees, to optimize data storage and retrieval efficiency.*	*Explore the basics of Wi-Fi technology, including standards, frequency bands, and security considerations, to understand its deployment and configuration.*	*Evaluate security concerns specific to social media platforms, identifying vulnerabilities and potential threats*	*Utilize tools and technologies for cybersecurity, understanding their application in safeguarding digital assets.*
SLO-8	*Participants will evaluate the legal aspects of I/O interface technologies, particularly interrupt and DMA modes, considering privacy and security regulations.*	*Analyze transactions and concurrency control mechanisms, including locking and timestamp-based protocols, to ensure data consistency in multi-user environments.*	*Investigate network security concepts, focusing on authentication mechanisms and their role in verifying the identities of users and devices.*	*Investigate various types of social networks and their characteristics, including their usage patterns and user demographics.*	*Implement effective password policies to enhance security measures and protect against unauthorized access.*
SLO-9	*Master of Law students will analyze the legal facets of processes, threads, inter-process communication, concurrency, and synchronization, addressing issues such as data privacy and contractual obligations.*	*Explore the concept of layering in networking protocols, understanding its role in organizing and abstracting communication functionalities.*	*Analyze the fundamentals of public key and private key cryptography, including encryption, decryption, and key management principles.*	*Scrutinize different social media platforms, understanding their features, functionalities, and target audiences.*	*Manage security patch deployment across digital devices to address vulnerabilities and ensure system integrity.*
SLO-10	*Tutorial – Conducting a scenario analysis on legal compliance with data protection regulations in the context of main memory and secondary storage.*	*Tutorial – Conduct an activity to analyze file organization strategies and their impact on query performance, comparing indexing techniques such as B and B+ trees.*	*Tutorial – Investigate common application layer protocols like DNS, SMTP, and HTTP, and their functionalities, with practical scenarios and troubleshooting activities.*	*Tutorial – Execute the marketing plan on selected social media platforms, utilizing features like sponsored posts, targeted ads, and influencer collaborations.*	*Tutorial –conduct an activity to explore endpoint device and mobile phone security.*
SLO-11	*Practice: Participating in a Judgment writing (dissent) and defend legal positions*	***Practice:** Participate in a practical exercise to implement and evaluate indexing techniques like B and B+ trees, aiming to gauge their effectiveness in improving query performance and optimizing data retrieval.*	***Practice:** Perform Wi-Fi site surveys to assess signal strength, interference, and coverage area in different environments.*	***Practice:** Execute a marketing strategy using social media platforms, tracking engagement metrics and analyzing campaign effectiveness.*	***Practice:** Install, configure, and test security tools to understand their functionality and effectiveness in threat detection and prevention.*

SLO-12	*Practice: Undertaking a research project on a selected emerging technology and its legal challenges*	***Practice** : Collaborate on exercises to implement and analyze concurrency control mechanisms, simulating scenarios of conflicting transactions and resolving them using locking protocols.*	***Practice:** Deploy security tools and techniques such as packet filtering and VPNs to mitigate security threats in a controlled environment.*	***Practice** Conduct a privacy audit to assess the privacy and security settings of a selected social media platform**.***	***Practice:** Design password complexity requirements, expiration policies, and multi-factor authentication guidelines to enhance security.*
SLO-13	*Learners will understand the legal considerations associated with deadlock situations, including contractual obligations and liability.*	*Evaluate LAN technologies, particularly Ethernet, including their protocols, addressing schemes, and collision detection mechanisms.*	*Examine digital signatures and certificates, understanding their role in ensuring data integrity, authenticity, and non-repudiation in network communications.*	*Assess social media monitoring techniques, including the use of hashtags and the detection of viral content.*	*Execute data backup procedures to mitigate the risk of data loss and ensure business continuity.*
SLO-14	*Students will analyze the legal aspects of CPU scheduling, considering issues such as fairness, discrimination, and contractual obligations.*	***Examine** flow and error control techniques, as well as switching methods, in data transmission over networks.*	*Evaluate the functionality and deployment of firewalls in network security architectures, assessing their role in preventing unauthorized access and protecting against cyber threats.*	*Explore social media marketing strategies, incorporating the utilization of social media platforms for branding, advertising, and enhancing customer engagement.*	*Evaluate the risks associated with downloading and managing third-party software, and adopt appropriate security measures.*
SLO-15	*Participants will examine the legal dimensions of memory management and virtual memory, addressing issues such as data protection, privacy, and contractual obligations.*	*Analyze IPv4/IPv6 protocols, routers, and routing algorithms (e.g., distance vector, link state), understanding their functionalities and roles in packet routing.*	*Assess network security challenges and solutions in contemporary environments, including emerging threats and mitigation strategies.*	*Appraise privacy issues related to social media usage, considering challenges and opportunities for maintaining user privacy online.*	*Develop and enforce device security policies to establish guidelines for secure device usage and management.*
SLO-16	*Tutorial: Conducting a simulated ethical dilemma scenario where students apply ethical guidelines to navigate a situation involving AI in legal practice.*	*Tutorial – Simulate routing scenarios using packet tracer or similar tools, evaluating the efficiency of different routing algorithms in various network topologies.*	*Tutorial – simulated network environment where users authenticate using passwords, implement encryption for data transmission, and configure firewall rules to control network access, followed by a simulated cyber attack scenario to assess the effectiveness of the implemented security measures.*	*Tutorial – Propose potential adjustments to strategy and tactics based on insights gathered from data analysis and audience responses.*	*Tutorial – Demonstrate how to use selected tools to gain familiarity with cybersecurity tools and technologies.*

SLO-17	*Practice: Engaging in a negotiation exercise involving technology contracts*	***Practice:** Attend a demonstration on LAN technologies, including Ethernet, where different protocols and collision detection mechanisms are illustrated and explained.*	***Practice:** Generate and manage cryptographic keys, create digital signatures, and verify certificate authenticity in practical exercises.*	***Practice:** Monitor social media platforms for trending topics and viral content using analytics tools*	***Practice:** Deploy security patches according to a patch management schedule, ensuring timely updates to mitigate vulnerabilities.*
SLO-18	*Practice: Presenting and discussing research on the societal impact of technology from a legal perspective*	***Practice:** Engage in a simulation activity to implement and compare routing algorithms like distance vector and link state, analyzing their efficiency and scalability in different network topologies.*	***Practice:** Test firewall configurations using penetration testing tools to identify and address vulnerabilities in network security defenses.*	***Practice:** Engage in structured debates, presenting arguments for and against various ethical dilemmas related to social media.*	***Practice:** Draft and implement a device security policy for an organization or personal use.*
Assessment	*Continuous Learning Assessment - 1*		*Continuous Learning Assessment - 2*		
	Continuous Learning Assessment - 3				

Resources			
1	Nina Godbole&SunitBelapure “Cyber Security”, Wiley India, 2022 Reprint	2	Bruce Newsome, “A Practical Introduction to Security and Risk Management”, 20203.
3	Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers.	4	David L. Cannon, “CISA Certified Information Systems Auditor Study Guide”, John Wiley & Sons
5	Cyber Crime Impact in the New Millennium, by R. C Mishra,Auther Press. Edition 2010.	6	Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by SumitBelapure and Nina God bole, Wiley India Pvt. Ltd. (First Edition, 2011).
7	Security in the Digital Age: Social Media Security Treats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform. (Pearson , 13th November, 2001)	8	Electronic Commerce by Elias M. Awad, Prentice Hall of India Pvt Ltd.
9	Electronic Commerce by Elias M. Awad, Prentice Hall of India Pvt Ltd.	10	Fundamentals of Network Security by E. Maiwald, McGraw Hill.

Rationale (CLR)	*The purpose of learning this course is to:*	Depth				Attainment			Program Learning Outcomes (PLO)											
		1	2	3	4	1	2	3	1	2	3	4	5	6	7	8	9	10	11	12
CLR-1	*Equip participants with an in-depth comprehension of computer architecture and operating systems, covering various aspects such as machine instructions, A LU functionality, memory hierarchy, process management, CPU scheduling, and file systems. Through this comprehensive understanding, learners will develop proficiency in designing, analyzing, and optimizing computing systems to meet diverse computational requirements efficiently.*																			
CLR-2	*Develop a comprehensive understanding of database systems and networking fundamentals, including ER and relational models, SQL, integrity constraints, file organization, indexing techniques, transactions, concurrency control, LAN technologies, flow control, IPv4/IPv6, routers, and routing algorithms, to facilitate adept database management and network administration.*																			
CLR-3	*Equip students with the ability to analyze TCP/UDP protocols, congestion control mechanisms, application layer protocols, Wi-Fi fundamentals, network security, cryptography basics, digital signatures, certificates, and firewall deployment, fostering a comprehensive understanding of network fundamentals.*																			
CLR-4	*Explore the fundamentals of cyberspace, computer and web technology, social media security, and marketing, assessing various social media platforms, monitoring techniques, and privacy challenges to foster a comprehensive understanding of online networks.*																			
CLR-5	*Empower participants with the expertise to effectively implement robust cybersecurity measures within e-commerce and digital payment ecosystems. By covering threat identification, security best practices, device protection, and policy formulation, learners will develop comprehensive skills essential for ensuring the security and integrity of online transactions.*																			

Outcomes (CLO)	*At the end of this course, learners will be able to:*	Conceive	Design	Implement	Operate	Level of Thinking	Expected Proficiency (%)	Expected Attainment (%)	Disciplinary Knowledge	Critical Thinking	Problem Solving	Analytical Reasoning	Research-related Skills	Communication Skills	Cooperation/Team Work	Digital Literacy	Self-directed Learning	Moral and Ethical Reasoning	Leadership Qualities	Life Long Learning
CLO-1	*Acquire a comprehensive understanding of computer architecture and operating systems, encompassing machine instructions, addressing modes, ALU functionality, instruction pipelining, memory hierarchy, I/O interfaces, process management, concurrency, CPU scheduling, memory management, virtual memory, and file systems, thus enabling proficiency in designing, analyzing, and optimizing computing systems.*	✓	✓		-	2	85	75	3	-	-	1	-	3	-	2	2	1	2	3
CLO-2	*Attain a comprehensive proficiency in database systems and networking fundamentals, covering ER and relational models, SQL, integrity constraints, normal forms, file organization, indexing techniques, transactions, concurrency control, layering concepts, LAN technologies, flow and error control techniques, as well as IPv4/IPv6, routers, and routing algorithms, facilitating adeptness in database management and network administration.*	✓	✓	✓	-	2	85	75	3	2	1	2	2	3	1	1	2	1	2	3
CLO-3	*Analyze TCP/UDP protocols, congestion control mechanisms, application layer protocols, Wi-Fi fundamentals, network security, cryptography basics, digital signatures, certificates, and firewall deployment for comprehensive understanding of network fundamentals.*	✓	✓	✓	✓	3	85	75	3	1	2	1	3	3	1	1	1	2	2	3
CLO-4	*Investigate the fundamentals of cyberspace, computer and web technology, social media security, and marketing, scrutinizing various social media platforms, monitoring techniques, and privacy challenges to cultivate a comprehensive understanding of online networks.*	✓	✓	✓	✓	3	85	75	3	3	2	3	3	3	-	2	3	3	3	3
CLO-5	*Master the implementation of robust cybersecurity measures across e-commerce and digital payment ecosystems, covering threat identification, security best practices, device protection, and effective policy formulation.*	✓	✓	✓	✓	3	85	75	3	3	2	3	3	3	-	2	3	3	3	3

Assessment Method (Max. Marks: 100)																	
		Continuous Learning Assessment (CLA 40% Weightage)												Final Exam			
Level of Thinking		Model Exam (20%)				Assignment/ Seminar/Group discussion/ Presentation				Participation in seminar/ Conference/ Publication				Participation in class room/co-curricular & Para curricular activities			
		(20%)				(10%)				(5%)				(5%)		(60%)	
1	Remember	40%		-		40%		-		30%		-			-	40%	-
2	Understand																
3	Apply	40%		-		40%		-		40%		-			-	40%	-
4	Analyze																
5	Evaluate	20%		-		20%		-		30%		-			-	20%	-
6	Create																
Total		100 %				100 %				100 %				100 %		100 %	

Strategies						
	Technology		Pedagogy / Andragogy		Sustainable Development	
	Simulations	✓	Clarification/Pauses	✓	Good Health & Well Being	✓
	Presentation Tools					
	Learning Management System	✓	Group Discussion	✓	Quality Education	✓
			Hands-on Practice	✓		
			Debate	✓		
			Interactive Lecture	✓		
			Brainstorming	✓		

Designers					
Professional Experts		Higher Institution Experts		Internal Experts	
1	*<name>, <industry name>, <email id>*	1	*<name>, <institution name>, <email id>*	1	*<name>, SRMIST, <email id>*
2	*<name>, <industry name>, <email id>*	2	*<name>, <institution name>, <email id>*	2	*<name>, SRMIST, <email id>*

Code	PLCS24104T	Title	INTRODUCTION TO CYBER SPACE, CYBER LAW AND SECURITY	Category		Professional Core	L	T	P	C
							3	1	2	5

Course Offering Department	School of Law	Pre-requisite Courses	Nil	Co-requisite Courses	Nil	Progressive Courses	Nil	Data Book / Codes/Standards	

Title & Content	Unit 1	Unit 2	Unit 3	Unit 4	Unit 5
Duration (hour)	18	18	18	18	18
SLO-1	*Develop a foundational understanding of cyber space, including its definition, components (computer and network), and the significance of the internet and online resources.*	*Attain a comprehensive understanding of the meaning, definition, and various types of e-commerce, emphasizing the legal nuances involved*	*Critically analyze and evaluate complex Intellectual Property Rights (IPR) issues, demonstrating an advanced understanding of the legal intricacies involved.*	*Achieve a nuanced comprehension of diverse regulatory frameworks, critically evaluating international and domestic legal regimes governing cyber activities.*	*Demonstrate an advanced understanding of cyber security, encompassing nuanced interpretations of meaning, advanced basics, and intricate concepts of secure infrastructure.*
SLO-2	*Gain comprehensive knowledge of cyber law, exploring its role, scope, and the regulatory frameworks governing activities in cyber space.*	*Develop expertise in managing legal aspects of cross-border e-commerce, addressing regulatory challenges and international trade considerations.*	*Demonstrate advanced expertise in dissecting intricate copyright dynamics in the digital scenario, examining emerging challenges and proposing sophisticated legal solutions.*	*Conduct advanced research on the international legal regime, examining key conventions such as the Hague Convention on Jurisdiction and Foreign Judgments and the European Convention on Cyber Crimes.*	*Conduct a critical analysis of sophisticated challenges in cyber security, showcasing an ability to comprehend and navigate complex issues.*
SLO-3	*Analyze the legal dimensions of e-commerce, understanding its regulation and the legal control mechanisms applicable to online business transactions.*	*Acquire proficiency in addressing identity management issues in the context of e-commerce, ensuring legal compliance and data security.*	*Conduct in-depth examinations of copyright infringement in cyberspace, employing advanced analytical skills to assess the nuances of linking, inclining, framing, and legal repercussions*	*Develop expertise in scrutinizing domestic legal regimes, emphasizing the application and implications of the Information Technology Act, 2000.*	*Demonstrate advanced proficiency in implementing security defenses, utilizing the NIST 800 framework and deploying various firewall types strategically by law*
SLO-4	*Tutorial: Analyze a recent cyber law case, discussing regulatory aspects and legal frameworks in cyber space.*	*Tutorial : Analyze cases, compare regulations, and develop compliance strategies for cross-border e-commerce, culminating in group presentations.*	*Tutorial: Engage PG students in an advanced workshop focusing on legal research methodologies for IPR issues in cyberspace, emphasizing critical analysis and application.*	*Tutorial : Explore international and domestic legal regimes, focusing on key conventions like Hague, European Cyber Crimes, and UNCITRAL Model Law.*	*Tutorial : Explore legal frameworks and implications in an advanced tutorial on cyber security*
SLO-5	*Practice: Students conduct an in-depth analysis of key cyber law legislations, examining their provisions, amendments, and relevant legal precedents.*	*Practice: Organize a symposium where students present their research findings on recent developments and legal challenges in e-commerce regulations, fostering discussions on emerging trends.*	*Practice: Organize a symposium for LLM students to present and discuss advanced legal research on contemporary challenges in digital copyright, fostering academic discourse.*	*Practice: Role-play different scenarios to apply the Hague Convention, European Cyber Crimes Convention, and UNCITRAL Model Law, exploring cross-border jurisdiction challenges*	*Practice: Engage students in a detailed analysis of legal frameworks and implications, encouraging critical thinking and advanced understanding.*

SLO-6	*Practice: Participants conduct legal research on the regulatory frameworks impacting e-commerce, focusing on recent changes, case law, and emerging trends.*	*Practice: Assign students different jurisdictions to conduct a comparative analysis of privacy and data protection legislation impacting e-commerce, highlighting key differences and implications.*	*Practice: Establish a research clinic for LL.M. scholars to investigate and analyze the evolving jurisprudence in digital copyright, emphasizing cutting-edge cases and legal developments.*	*Practice: Conduct a mock IPR clinic where participants analyze real-world cases under Berne Convention, WIPO Copyright Treaty, and the OECD Convention on Database Protection.*	*Practice: Conduct a hands-on simulation where students formulate legal strategies for cyber defense, applying NIST 800 framework and firewall types within a legal context.*
SLO-7	*Comprehend the legal aspects of online contracts, exploring the mechanisms for their regulation and enforcement in the digital environment.*	*Conduct legal analyses of issues related to access in e-commerce, considering factors such as digital accessibility and legal barriers.*	*Navigate the nuanced balance between copyright protection and freedom of expression at an advanced level, critically assessing reasonable restrictions and their extensive applicability.*	*Undertake comprehensive research on the Hague Convention on Jurisdiction and Foreign Judgments, delving into its nuances and impact on cross-border legal issues*	*Navigate the legal aspects of securing wireless networks, addressing vulnerabilities strategically within the framework of cyber law.*
SLO-8	*Evaluate the legal frameworks governing social media, understanding issues related to privacy, defamation, and content control in the realm of cyber space*	*Master the legal dimensions of privacy and data protection in e-commerce, addressing compliance with data protection laws and safeguarding consumer information.*	*Attain advanced proficiency in conceptualizing trademarks in the digital realm, showcasing an in-depth understanding of their roles and implications.*	*Conduct a critical assessment of the UNCITRAL Model Law on Electronic Commerce 1996, exploring its significance and effectiveness in regulating electronic transactions.*	*Analyze the legal implications of crafting Intrusion Detection System (IDS) signatures, considering privacy, data protection, and legal compliance.*
SLO-9	*Delve into the complexities of IPR in cyber space, examining issues connected with copyright, trademarks, and software patenting.*	*Gain insights into the legal complexities of e-commerce taxation and contractual issues, understanding their impact on businesses and consumers.*	*Demonstrate sophisticated skills in analyzing trademark infringement issues specific to cyberspace, unraveling the legal intricacies surrounding domain names.*	*Conduct advanced academic research on the legal control mechanisms of Intellectual Property Rights, including conventions such as the Berne Convention and the WIPO Copyright Treaty.*	*Explore the legal considerations surrounding monitoring and logging techniques for threat detection, focusing on privacy laws and legal compliance.*
SLO-10	*Tutorial: Simulate a hypothetical e-commerce scenario to explore legal considerations, contracts, and taxation challenges.*	*Tutorial: Assign scenarios, have students draft e-commerce contracts, engage in peer review, and facilitate class discussion on challenges and revisions.*	*Tutorial: Conduct a tutorial exploring sophisticated strategies for protecting trademarks in digital realms, covering advanced concepts, case studies, and regulatory considerations.*	*Tutorial – Dive into the legal intricacies of IPR, including Berne Convention, WIPO Copyright Treaty, and the OECD Convention on Database Protection.*	*Tutorial – Conduct a workshop guiding students in formulating legal strategies for security defenses aligned with the NIST 800 framework and various firewalls.*
SLO-11	*Practice: Groups delve into legal literature and court decisions related to social media, creating a summary of key legal principles and implications for users and platforms.*	*Practice: Establish a research forum where students delve into the complexities of e-commerce taxation laws, presenting their findings on global and regional tax implications for online businesses..*	*Practice: Simulate cross-border IPR negotiations, challenging LLM students to navigate complex legal issues, negotiate agreements, and analyze the implications of international law..*	*Practice: Organize a research symposium where students present findings on cyber conventions, encouraging academic discussion and collaboration.*	*Practice: conduct an interactive workshop focusing on legal leadership in GRC within cyber security, guiding students in audit management and legal considerations.*
SLO-12	*Practice: Learners explore jurisdictional nuances in intellectual property rights (IPR) cases in cyber space, examining*	*Practice: Conduct a jurisprudence review session where students explore landmark cases shaping Intellectual Property Rights (IPR)*	*Practice: Thematic Legal Writing Workshop: Crafting Advanced Writings on the Intricate Relationship Between IPR and*	*Practice: Engage in a hands-on workshop exploring practical applications of the OECD Convention on Database*	*Practice: Organize a debate-style activity where students discuss and analyze legal perspectives on emerging cybersecurity*

	legal decisions and comparing approaches in different jurisdictions.	*in e-commerce, analyzing legal principles and implications.*	*Digital Expression for LL.M. Candidates.*	*Protection, addressing data protection and intellectual property concerns.*	*challenges, fostering critical legal analysis.*
SLO-13	*Explore the legal implications of e-governance, understanding the role of legal frameworks in ensuring accountability and transparency in government digital initiatives.*	*Develop legal competence in addressing issues related to Intellectual Property Rights (IPR) in the context of e-commerce, including copyright, trademarks, and patents.*	*Attain an expert-level understanding of the interactions between domain names and trademarks, critically analyzing legal regulations at both international and domestic levels.*	*Undertake an in-depth exploration of the OECD Convention on Database Protection, evaluating its implications on data protection and intellectual property*	*Examine the legal frameworks governing the implementation of cryptography, emphasizing encryption laws, data protection, and legal constraints.*
SLO-14	*Analyze the legal aspects of e-taxation, exploring the regulatory landscape and legal challenges associated with taxing digital transactions.*	*Attain proficiency in legal frameworks for consumer protection in e-commerce, ensuring fair practices and addressing disputes.*	*Exhibit advanced legal research competence, delving deeply into international and domestic regulations governing IPR, trademarks, and copyright in cyberspace.*	*Perform an analytical study of the Rome Convention, examining its impact on choice of law in international contracts, particularly in the digital realm.*	*Apply the MITRE ATT&CK framework from a legal standpoint, considering legal implications and compliance in assessing and mitigating security vulnerabilities.*
SLO-15	*Comprehensive understanding of the Information Technology Act, 2000, examining its provisions and implications for legal practices in cyber space.*	*Develop awareness of jurisdictional issues in e-commerce and acquire skills in international trade dispute resolution, considering legal frameworks and mechanisms.*	*Showcase an advanced appreciation of the multifaceted roles played by both public and private international law in shaping legal frameworks and resolving intricate cross-border IPR issues.*	*Develop expertise in the WIPO Copyright Treaty and the Uniform Domain-Name Dispute-Resolution Policy (UDRP), analyzing their roles in protecting intellectual property and resolving domain disputes.*	*Showcase advanced legal leadership in Governance, Risk & Compliance (GRC), emphasizing audit management and a deep understanding of the legal aspects of the Indian cyber security system.*
SLO-16	*Tutorial: Facilitate a discussion on intellectual property rights in cyber space, analyzing legal frameworks and fostering insights through a roundtable format.*	*Tutorial: Simulate an e-commerce dispute, assign roles (lawyers, mediators), and engage in negotiation, mediation, or arbitration, followed by a debrief and analysis.*	*Tutorial: Facilitate a seminar guiding students through complex cross-border IPR dispute resolution scenarios, applying advanced legal principles and examining international frameworks.*	*Tutorial: Examine legal aspects of domain disputes, analyzing the Rome Convention and delving into expertise-building on WIPO Copyright Treaty and UDRP.*	*Tutorial: conduct a seminar focusing on legal leadership in GRC within cyber security, emphasizing audit management and legal aspects of the Indian cyber security system.*
SLO-17	*Practice: Students perform legal research to identify relevant legal precedents and case law shaping the legal landscape of e-governance, with a focus on government initiatives and legal challenges.*	*Practice: Facilitate a roundtable discussion focused on legal research in consumer protection within e-commerce, encouraging students to share insights, challenges, and potential research directions.*	*Practice: International Dispute Resolution Symposium on Cyber IPR Cases: LL.M. Participants Analyze Complex Cases and Propose Innovative Resolutions.*	*Practice: Simulate domain dispute resolution scenarios applying principles from the Rome Convention and practicing resolution mechanisms such as UDRP.*	*Practice: Conduct a workshop exploring the legal implications of crafting IDS signatures, emphasizing privacy, data protection, and legal compliance.*
SLO-18	*Practice: Participants engage in legal research to benchmark cyber security compliance standards, exploring legal guidelines, industry best practices, and recent legal developments in the cyber security domain.*	*Practice: Assign students to analyze legal precedents related to corporate liability in e-commerce, emphasizing cases that have shaped legal doctrines and liability standards.*	*Practice: Advanced Roundtable on Privacy and Data Protection Laws in E-commerce: In-depth Discussions Among LL.M. Students on the Evolving Legal Landscape.*	*Practice: Participate in a legislative drafting challenge where students draft sections aligning with international and domestic legal regimes, fostering practical legislative skills.*	*Practice: Engage students in an exercise highlighting legal considerations in monitoring and logging techniques for threat detection, ensuring compliance with privacy laws.*

Assessment	*Continuous Learning Assessment - 1*	*Continuous Learning Assessment - 2*
	Continuous Learning Assessment - 3	

Resources			
1	Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd.	6	Information Warfare and Security by Dorothy F. Denning, Addison Wesley.
2	Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform.	7	Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd.
3	Data Privacy Principles and Practice by Natraj Venkataramanan and Ashwin Shriram, CRC Press.	8	Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers.
4	Information Security Governance, Guidance for Information Security Managers by W. KragBrothy, 1st Edition, Wiley Publication.	9	Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform. (Pearson , 13th November, 2001)
5	Auditing IT Infrastructures for Compliance by Martin Weiss, Michael G. Solomon, 2nd Edition, Jones Bartlett Learning.	10	Fundamentals of Network Security by E. Maiwald, McGraw Hill.

Rationale (CLR)	*The purpose of learning this course is to:*	Depth				Attainment			Program Learning Outcomes (PLO)											
		1	2	3	4	1	2	3	1	2	3	4	5	6	7	8	9	10	11	12
CLR-1	*Advanced expertise in cyber law, covering essential aspects such as cyber space definitions, internet regulations, e-commerce, online contracts, social media governance, IPR challenges, e-governance, e-taxation, and a profound understanding of the Information Technology Act, 2000. The curriculum is designed to provide both theoretical insights and practical skills necessary for navigating and addressing legal complexities in the rapidly evolving digital landscape.*																			
CLR-2	*Elevate legal proficiency across Cyber Security, Regulatory Frameworks, Intellectual Property Rights, and E-commerce. It aims to cultivate a nuanced understanding of complex legal issues, encourage strategic application of legal frameworks, and develop leadership skills to navigate contemporary challenges in the dynamic legal landscape*																			
CLR-3	*Attaining advanced expertise in Intellectual Property Rights (IPR) with a deep dive into intricate aspects, including copyright challenges in the digital realm, cyberspace infringement issues, domain names, trademarks, and nuanced comprehension of legal regulations at both international and domestic levels. Emphasis is placed on understanding the influential role of public and private international law in shaping legal frameworks.*																			
CLR-4	*Cultivate advanced legal proficiency by mastering international and domestic regulatory frameworks and conventions, including Hague, European Cyber Crimes, and UNCITRAL Model Law. Students will develop expertise in Intellectual Property Rights (IPR) control, database protection, and cyber law legislations, fostering a comprehensive understanding of the Information Technology Act, 2000, to navigate intricate legal landscapes effectively.*																			
CLR-5	*Cultivates advanced legal proficiency, mastering global and local regulatory frameworks like Hague, European Cyber Crimes, and UNCITRAL. Students develop expertise in IPR, database protection, and cyber law (IT Act, 2000), enhancing skills to navigate intricate legal landscapes effectively.*																			

Outcomes (CLO)	*At the end of this course, learners will be able to:*	Conceive	Design	Implement	Operate	Level of Thinking	Expected Proficiency (%)	Expected Attainment (%)	Disciplinary Knowledge	Critical Thinking	Problem Solving	Analytical Reasoning	Research-related Skills	Communication Skills	Cooperation/Team Work	Digital Literacy	Self-directed Learning	Moral and Ethical Reasoning	Leadership Qualities	Life Long Learning
CLO-1	*Develop advanced legal expertise in cyber law, covering cyber space definitions, internet regulations, e-commerce, online contracts, social media governance, IPR challenges, e-governance, e-taxation, and a deep understanding of the Information Technology Act, 2000.*	✓	✓		-	2	85	75	3	2	-	1	-	3	-	2	2	1	2	3
CLO-2	*Attain advanced legal proficiency across diverse domains including Cyber Security, Regulatory Frameworks, Intellectual Property Rights, and E-commerce, fostering a nuanced understanding of complex legal issues, strategic application of legal frameworks, and leadership in navigating contemporary challenges in the evolving legal landscape.*	✓	✓	✓	-	2	85	75	3	2	1	2	2	3	-	1	2	1	2	3
CLO-3	*Attain advanced expertise in Intellectual Property Rights (IPR), delving into intricate aspects such as copyright challenges in the digital realm, cyberspace infringement issues, domain names, trademarks, and nuanced comprehension of legal regulations at both international and domestic levels, including the influential role of public and private international law in shaping legal frameworks.*	✓	✓	✓	✓	3	85	75	3	1	3	1	3	3	-	1	1	2	1	3
CLO-4	*Cultivate advanced legal proficiency by mastering international and domestic regulatory frameworks, conventions like Hague, European Cyber Crimes, and UNCITRAL Model Law. Develop expertise in Intellectual Property Rights (IPR) control, database protection, and cyber law legislations, including a comprehensive understanding of the Information Technology Act, 2000*	✓	✓	✓	✓	3	85	75	3	3	2	3	3	3	-	2	3	3	3	3
CLO-5	*This course aims to cultivate advanced legal proficiency by mastering international and domestic regulatory frameworks and conventions, including Hague, European Cyber Crimes, and UNCITRAL Model Law. Students will develop expertise in Intellectual Property Rights (IPR) control, database protection, and cyber law legislations, fostering a comprehensive understanding of the Information Technology Act, 2000, to navigate intricate legal landscapes effectively.*	✓	✓	✓	✓	3	85	75	3	3	2	3	3	3	-	3	3	3	3	3

Assessment Method (Max. Marks: 100)												
		Continuous Learning Assessment (CLA 40% Weightage)								Final Exam		
Level of Thinking		Model Exam (20%)		Assignment/ Seminar/Group discussion/ Presentation		Participation in seminar/ Conference/ Publication		Participation in class room/co-curricular & Para curricular activities				
		(20%)		(10%)		(5%)		(5%)		(60%)		
1	Remember	40%	-	40%	-	30%	-		-	40%	-	
2	Understand											
3	Apply	40%	-	40%	-	40%	-		-	40%	-	
4	Analyze											
5	Evaluate	20%	-	20%	-	30%	-		-	20%	-	
6	Create											
Total		100 %		100 %		100 %		100 %		100 %		

Strategies					
Technology		Pedagogy / Andragogy		Sustainable Development	
Simulations	✓	Clarification/Pauses	✓	Good Health & Well Being	✓
Presentation Tools	✓				
Learning Management System		Group Discussion	✓	Quality Education	✓
		Hands-on Practice	✓		
		Debate	✓		
		Interactive Lecture	✓		
		Brainstorming	✓		

Designers					
Professional Experts		Higher Institution Experts		Internal Experts	
1	*<name>, <industry name>, <email id>*	1	*<name>, <institution name>, <email id>*	1	*<name>, SRMIST, <email id>*
2	*<name>, <industry name>, <email id>*	2	*<name>, <institution name>, <email id>*	2	*<name>, SRMIST, <email id>*

Code	PLCS24201T	Title	JUDICIAL PROCESS	Category		Professional Core	L	T	P	C
							3	1	2	5

Course Offering Department	School of Law	Pre-requisite Courses		Co-requisite Courses		Progressive Courses		Data Book / Codes/Standards	

Title & Content	NATURE OF JUDICIAL PROCESS	DIMENSIONS OF JUDICIAL PROCESS	JUDICIAL PROCESS IN INDIA	JUDICIAL PROCESS IN CONSTITUTIONAL AMENDMENT	JUDICIAL ADMINISTRATION
Duration (hour)	18	18	18	18	18
SLO-1	*Comprehend the stages and key components of judicial process, including initiation of legal action,pleadings,discovery,final,verdict, judgment,appeals ,enforcement of judgements.*	*Explain and comprehend different methods of interpretation to interpret law to ensure consistency and fairness in decision making.*	*Examine the structure of the judicial system in India including the hierarchy of courts, its jurisdiction and function at each level of judiciary .*	*Comprehend and analyze the rationale behind the doctrine of Prospective overruling and its implications for legal certainty, stability, and the rule of law.*	*Comprehend the process of selection and appointment of Judges* in district court, high court and supreme court of India .
SLO-2	*Examine the concepts of law,justice,ethics and morality including their interrelationships and distinctions*	*Examine the approaches and methodology employed in constitutional interpretation of the civil law and common law countries*	*Comprehend the system of alternative adjudication in India such as mediation, arbitration, and conciliation, as alternatives to traditional litigation*	*Examine and analyze the doctrine of colourable legislation*	*Examine the policies and procedures governing the transfer of judges within the judiciary, including the reasons for transfers and the mechanisms for ensuring transparency and fairness in the transfer process.*
SLO-3	*Analyze the intersection of legal decisions with ethical and moral considerations and how justice is sought through legal mechanisms*	*Comprehend the approaches and methodology employed in the statutory interpretation of civil law and common law countries .*	*Gain comprehensive understanding of the structure, jurisdiction, and effectiveness of Nyaya Panchayats in providing access to justice and resolving disputes at the grassroots level.*	*Gain a comprehensive understanding of the doctrine of harmonious interpretation and its role in reconciling conflicting provisions within statutes or constitutional provisions .*	*Analyze the importance of manpower planning in ensuring the effective functioning of the judiciary, including the allocation of human and financial resources.*
SLO-4	*Tutorial: Conduct an in depth discussion on law,justice,ethics and morality .*	*Tutorial: Conduct an in depth discussion on the comprehensive understanding of methods of interpretation*	*Tutorial: Conduct an in depth discussion of advantages and limitations of alternative adjudication and its role in reducing the burden on the formal judicial system*	*Tutorial: Conduct an in depth discussion on the doctrines of constitutional interpretation*	*Tutorial: Conduct an in depth discussion on recent appointment and transfer of judges in high courts and supreme court of India*

SLO-5	*Practice: Evaluate and analyze hypothetical legal scenarios by applying the ethical considerations and reasoning techniques.*	*Practice: Evaluate different legal scenarios by employing different types of interpretation .*	*Practice: Engage in case studies involving landmark cases of alternative adjudication in India.*	*Practice: Engage in case studies involving landmark cases of prospective overruling .*	*Practice: Discuss the impact of transfer policies on judicial independence, efficiency, and accountability.*
SLO-6	*Practice: Engage in making well reasoned arguments and making sound legal judgements based on relevant laws,precedents and ethical norms.*	*Practice: Explore and differentiate between different methods of interpretation in civil and common law countries.*	*Practice: Classroom application of alternative dispute resolution methods for hypothetical cases.*	*Practice: Engage in case studies involving landmark cases of colourable legislation, harmonious construction .*	*Practice: Discuss the challenges and considerations involved in manpower planning, such as budget constraints, staffing levels,and workload distribution.*
SLO-7	*Comprehend the various components of legal reasoning and examine application of these reasoning to analyze legal issues and construct persuasive arguments.*	*Analyze the concept of judicial review and its importance in analyzing the constitutionality of laws.*	*Gain an understanding of the evolution of public interest litigation/ social interest litigation in india.*	*Comprehend and analyze other doctrines including pith and substance .*	*Examine the legal framework governing judicial impact assessment as a tool for evaluating the potential impact of judicial decisions, legislation, or policy changes on the judiciary and the legal system.*
SLO-8	*Discuss and understand deductive reasoning, inductive reasoning and dialectical reasoning .*	*Examine the concept of judicial activism, proactive role of judges in shaping individual rights and progressive social change.*	*Examine the procedural aspects of public interest litigation/ social interest litigation, including standing, locus standi, and the role of public interest petitioners and interveners.*	*Examine and analyze the origins, development, and significance of the Doctrine of Basic Structure theory in constitutional jurisprudence.*	*Analyze the methodology and process of conducting Judicial Impact Assessment and its role in promoting transparency, accountability, and evidence-based decision-making.*
SLO-9	*Comprehend the concept of analogy , reasoning by comparison to similar cases.*	*Comprehend the concept of judicial restraint*	*Gain an understanding of landmark public interest litigation/ social interest litigation cases and their impact on social justice, human rights, environmental protection, and governance in India.*	*Analyze the recent judicial decisions and developments related to the Doctrine of Basic Structure Theory, including its application to specific constitutional provisions and issues.*	*Examine the factors contributing to mounting arrears in the judicial system, such as backlog of cases, delays in court proceedings, and inefficiencies in case management.*
SLO-10	*Tutorial: Conduct in depth discussion on methods of legal reasoning.*	*Tutorial: Conduct an in depth discussion on the proactive role of the judges through judicial activism as against the conventional separation of powers.*	*Tutorial: Conduct an in depth discussion on public interest litigation in Indian jurisprudence*	*Tutorial –.Conduct an in depth discussion on the basic structure doctrine and amendment of constitution.*	*Tutorial – Conduct an in depth discussion on the judicial impact assessment.*

SLO-11	*Practice: Engage in giving illustration of cases to apply general principles to specific cases and specific principles to general cases.*	*Practice: Discuss in case studies involving judicial review .*	*Practice: Engage in case studies involving landmark cases of public interest litigation.*	*Practice: Engage in case discussion of Kesavananda Bharathi v state of kerala*	*Practice: Discuss the potential effects of judicial decisions on various stakeholders and the broader legal system.*
SLO-12	*Practice: Engage in giving illustration of cases by comparison to similar cases to understand the concept of analogy*	*Practice: Discuss in case studies involving judicial activism and judicial restraint*	*Practice: Engage in the classroom drafting of public interest litigation petitions .*	*Practice: Engage in case discussion of other cases relating to basic structure doctrine.*	*Practice: Examine the practical consequences of mounting arrears on access to justice, judicial efficiency, and public confidence in the legal system.*
SLO-13	*Explore the tools and techniques employed by judges to creatively interpret laws to balance the competing interests*	*Explain the principles of judicial accountability,transparency and independence of judiciary as an essential component of fair and impartial judiciary.*	*Comprehend the concept of judicial policy-making and its role in shaping legal doctrines, principles, and public policy.*	*Comprehend and analyze the process of constitutional amendment in india*	*Examine the patterns of court management, such as case-flow management, docket management, and alternative dispute resolution mechanisms.*
SLO-14	*Comprehend the ethical and practical implications in judicial creativity in promoting fairness and justice within the legal system.*	*Comprehend the mechanisms for promoting judicial accountability and transparency, such as judicial codes of conduct, judicial performance evaluations, and public access to court proceedings and records.*	*Gain an understanding of the evolution of doctrines and principles in India*	*Comprehend the process of constitutional amendment in America, the historical context of constitutional amendments and their impact on civil rights, governance, and federalism.*	*Explore the recommendations made by the Law Commission or similar bodies relating to court management, reforming the judiciary and improving the administration of justice.*
SLO-15	*Explore the importance of precedents in the common law system and how it operates as a source of legal authority in providing guidance to courts in similar cases.*	*Gain an understanding of the Bangalore principles of judicial conduct aimed at promoting judicial integrity*	*Gain an understanding of the landmark judgments and legal developments that have contributed to the evolution of Indian legal principles and doctrines over time.*	*Examine, compare and distinguish the constitutional amendment process in different legal systems such as India and America .*	*Examine and analyze the national case management system in India including the E court system in India .*
SLO-16	*Tutorial: Conduct in depth discussion on the tools and techniques of judicial creativity and its role in shaping legal principles and doctrines*	*Tutorial: Conduct an in depth discussion on judicial integrity .*	*Tutorial: Conduct an in depth* analysis and discussion on, judicial policy-making, and the evolution of legal doctrines and principles.	*Tutorial: Discuss the step-by-step walkthrough of the amendment process in India and USA, and the potential exemptions.*	*Tutorial: Discuss in detail the Lord Woolf's Report on "Case Management" (UK)- Australian Law Reform Commission on "Judicial and case Management"*

SLO-17	*Practice: Discuss on landmark cases illustrating the interpretation and application of these principles.*	*Practice:* Discuss the role of judges in safeguarding the rule of law and judicial integrity .	*Practice: Engage in discussion on landmark cases related to legal doctrine in india*	*Practice: Discuss landmark cases pertaining to constitutional amendment in the USA .*	*Practice: Discuss the practical feasibility and effectiveness of these recommendations in addressing systemic challenges and promoting judicial efficiency and accountability.*
SLO-18	*Practice: Discuss the case studies to understand the doctrine of precedent*	*Practice:* Discuss the key principles outlined in the Bangalore Principles and their relevance to ensuring judicial independence, impartiality, integrity, and competence.	*Practice: Discuss the ethical considerations and professional responsibilities involved in judicial decision-making, policy formulation, and legal advocacy.*	*Practice: Discuss case studies pertaining to constitutional amendment in India.*	*Practice: Discuss the concept of master of roaster in India*

Resources			
1	*A. Lakshminath, "Precedent in Indian Law: Judicial Process" EBC Publication (2009*	2	*Aharon Barak, The Judge in a Democracy (Princeton University Press, 2008)*
3	*S.P. Sathe, Judicial Activism in India: Transgressing Borders and Enforcing Limits (2003)*	4	*Bernard C. Gavit, Ralph F. Fuchs, Cases and Materials on an Introduction to Law and the Judicial Process (1952)*
5	*Mauro Cappellletti, The Judicial Process in Comparative Perspective (Clarendon Press: Oxford, 1989).*		

Rationale (CLR)	*The purpose of learning this course is to:*	Depth				Attainment			Program Learning Outcomes (PLO)											
		1	2	3	4	1	2	3	1	2	3	4	5	6	7	8	9	10	11	12
CLR-1	*Enable participants to gain a comprehensive understanding of the judicial process, including the inquiry into law, justice, ethics, and morality. To explore the components of legal reasoning, such as deductive, inductive, analogy, and dialectical reasoning, along with the tools and techniques of judicial creativity and precedent.*	*Conceive*	*Design*	*Implement*	*Operate*	*Level of Thinking*	*Expected Proficiency (%)*	*Expected Attainment (%)*	*Disciplinary Knowledge*	*Critical Thinking*	*Problem Solving*	*Analytical Reasoning*	*Research-related Skills*	*Communication Skills*	*Cooperation/Team Work*	*Digital Literacy*	*Self-directed Learning*	*Moral and Ethical Reasoning*	*Leadership Qualities*	*Life Long Learning*
CLR-2	*To provide participants with an understanding of various methods of interpretation, including constitutional interpretation and statutory interpretation in civil and common law countries. To explore concepts such as judicial review, judicial activism, judicial self-restraint, judicial accountability, transparency, and independence, with a focus on the Bangalore Principles.*																			
CLR-3	*Provide participants with a comprehensive understanding of the structure of the judicial system in India, alternative methods of adjudication such as Nyaya Panchayats, the judicial process, Public Interest Litigation (PIL) or Social Action Litigation (SAL), judicial policy-making, and the evolution of legal doctrines and principles.*																			
CLR-4	*Equip participants with a deep understanding of legal doctrines and principles, including the Doctrine of Prospective Overruling, Colorable Legislation, Harmonious Interpretation, the Doctrine of Basic Structure Theory, Recent Developments in this theory, and the position of Constitutional Amendment in America.*																			
CLR-5	*Equip participants with comprehensive understanding of various aspects related to the selection and appointment of judges, transfer policies, manpower planning including finance, Judicial Impact Assessment (JIA), mounting arrears in courts, workload management, patterns of court management, and recommendations made by the Law Commission.*																			
Outcomes (CLO)	*At the end of this course, learners will be able to:*																			
CLO-1	*Gain a comprehensive understanding of the judicial process, legal reasoning, and the ethical dimensions of law and justice, enabling them to navigate complex legal issues with analytical rigor and ethical awareness.*	□	□		-	*2*	*85*	*75*	*3*	*-*	*-*	*1*	*-*	*3*	*-*	*2*	*2*	*1*	*2*	*3*
CLO-2	*Acquire understanding about various methods of interpretation employed by courts, the dynamics of judicial decision-making, and the broader issues of judicial accountability, transparency, and independence.Also, analyze legal issues, assess judicial decisions, and contribute to discussions on judicial reform and governance.*	□	□	□	-	*2*	*85*	*75*	*3*	*2*	*1*	*2*	*2*	*3*	*-*	*1*	*2*	*1*	*2*	*3*
CLO-3	*Gain comprehensive understanding about the functions of judiciary, the role of courts in promoting access to justice and social change, and understand the challenges and opportunities for judicial reform and development. To understand the complexities of the legal system and its impact on society, governance, and development.* .	□	□	□	□	*3*	*85*	*75*	*3*	*1*	*3*	*1*	*3*	*3*	*-*	*1*	*1*	*2*	*1*	*3*
CLO-4	*Develop a nuanced understanding of key legal doctrines, principles, and theories, enabling them to critically analyze constitutional issues,legal issues, interpret statutes, engage in informed debates, and contribute to the development of constitutional jurisprudence and legal reform.*	□	□	□	□	*3*	*85*	*75*	*3*	*3*	*2*	*3*	*3*	*3*	*-*	*2*	*3*	*3*	*3*	*3*
CLO-5	*Comprehend the challenges in judicial administration and management, also, to contribute to the development and implementation of policies and reforms aimed at enhancing the efficiency, accessibility, and accountability of the judiciary.*	□	□	□	□	*3*	*85*	*75*	*3*	*3*	*2*	*3*	*3*	*3*	*-*	*3*	*3*	*3*	*3*	*3*

Assessment Method (Max. Marks: 100)																	
		Continuous Learning Assessment (CLA 40% Weightage)												Final Exam			
Level of Thinking		Model Exam (20%)				Assignment/ Seminar/Group discussion/ Presentation				Participation in seminar/ Conference/ Publication				Participation in class room/co-curricular & Para curricular activities			
		(20%)				(10%)				(5%)				(5%)		(60%)	
1	Remember	40%		-		40%		-		30%		-			-	40%	-
2	Understand																
3	Apply	40%		-		40%		-		40%		-			-	40%	-
4	Analyze																
5	Evaluate	20%		-		20%		-		30%		-			-	20%	-
6	Create																
Total		100 %				100 %				100 %				100 %		100 %	

Strategies					
Technology		Pedagogy / Andragogy		Sustainable Development	
Simulations	✓	Clarification/Pauses	✓	Good Health & Well Being	✓
Presentation Tools	✓				
Learning Management System		Group Discussion	✓	Quality Education	✓
		Hands-on Practice	✓		
		Debate	✓		
		Interactive Lecture	✓		
		Brainstorming	✓		

Designers					
Professional Experts		Higher Institution Experts		Internal Experts	
1		1	DR. REDDIVARI REVATHI (Former HOD , Department of constitutional law , in School of Excellence in Law)	1	*Ms G. Bhavani, Assistant Professor, School of Law, SRMIST*
2		2	DR. MANJULA , Assistant Professor, School of Excellence in Law	2	

Code	PLCS24202T	Title	CYBER CRIMES & CYBER SECURITY	Category		Professional Core	L	T	P	C
							3	1	2	5

Course Offering Department	School of Law	Pre-requisite Courses		Co-requisite Courses		Progressive Courses		Data Book / Codes/Standards	

Title & Content	Unit 1	Unit 2	Unit 3	Unit 4	Unit 5
Duration (hour)	18	18	18	18	18
SLO-1	*Define the concept of cybercrime and identify its key characteristics.*	*Define crimes against state and government, including examples of such crimes and their legal implications.*	*Define and differentiate various types of cybercrimes such as cyberbullying, cyberstalking, phishing, cyberfraud, cybertaxation, spyware, e-mail spoofing, spamming, voyeurism, e-mail bombing, verbal attacks, clone attacks, flood attacks, cyberpornography, child pornography, social media frauds, online drug trafficking, cyber extortion, online recruitment fraud, cybercrimes against women, harassment via emails, and morphing.*	*Define and explain various types of cybercrimes against property such as computer trespassing, dissemination of viruses, hacking the network, website access by unauthorized parties, credit card fraud, disk loading, counterfeit software, internet time theft, and cybersquatting.*	*Identify and explain the key provisions and objectives of the Council of Europe's Convention on Cybercrime (2001), including its role as an international treaty aimed at addressing cybercrime through cooperation among states.*
SLO-2	*Explain the process of criminalizing certain conduct in cyberspace, including the role of legislation and case law.*	*Explain the concept of cyber warfare, its key ingredients, different types, and common perpetrators involved in carrying out these attacks.*	*Explain the psychological, emotional, and social impact of cyberbullying and cyberstalking on victims, including children and adolescents.*	*Identify and analyze the elements of each type of cybercrime against property, including any legal definitions or requirements for prosecution.*	*Analyze the significance of the Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist or Xenophobic Nature Committed Through Computer Systems (2003) in promoting human rights online and preventing hate speech.*

SLO-3	*Analyze the various behaviors that constitute cybercrimes, such as hacking, phishing, identity theft, and fraud.*	*Analyze the motivations and targets of various forms of cyber warfare, and evaluate the potential impact on national security.*	*Identify the legal and ethical implications of engaging in cyberdefamation or cyber smearing, and understand the consequences of spreading false information about others online.*	*Explain the impact of cybercrimes against property on individuals, businesses, and society as a whole.*	*Evaluate the impact of the Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence (2022) on cross-border investigations and information sharing between countries.*
SLO-4	*Tutorial: Seminar on Criminological Perspectives of Cybercrimes*	*Tutorial: Group Discussion on the Need for a clear definition of Cyberwarfare.*	*Tutorial: Seminar on the Evolving Aspects of Cyberdefamation in India.*	*Tutorial: Seminar on the broader societal implications of cybercrimes against property on individuals, businesses, such as effects on trust, security, and innovation.*	*Tutorial: Seminar on the Potential to Misuse Computer Systems to Propagate Racist and Xenophobic Ideas*
SLO-5	*Practice: Analyze how judges can influence legal norms regarding digital activities based on their rulings in specific cases.*	*Practice: Research upon cyber attacks in the past decade and list down how many of them have been perpetrated by State actors and non-State actors respectively.*	*Practice: Perform an ILAC analysis on problem scenarios in situations that could potentially be classified as one of the listed cybercrimes.*	*Practice: Gather key statistics or case studies demonstrating the economic impact of cybercrimes on organizations and write a report on the incidence of these cybercrimes in India.*	*Practice: Write an essay on the need for balancing between freedom of expression and effectively fighting against acts of a racist and xenophobic nature.*
SLO-6	*Practice: Write a short note on how cybercrimes are different from other crimes, considering factors like mens rea, actus reus, and stages of commission of a crime.*	*Practice: List down some common types of cyber warfare including espionage, economic disruption, propaganda attacks, power grid disruptions, etc., and explain their implications on day to day human life of the victim State's people.*	*Practice: Write a note on how AI has the tendency to aggravate or increase ease of facilitation of cybercrimes.*	*Practice: Identify the key elements that constitute cybercrimes against property discussed in this unit and explain how they meet the definition of the specific cybercrime*	*Practice: Write an overview of the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist or Xenophobic Nature Committed Through Computer Systems (2003) and its objectives.*
SLO-7	*Evaluate the complexities involved in determining jurisdiction over cybercrimes, including territorial, personal, and subject matter jurisdiction.*	*Differentiate between cyber warfare and cyber terrorism, highlighting the unique features and challenges associated with each phenomenon.*	*Analyze the risks and vulnerabilities associated with phishing scams, and develop strategies for identifying and avoiding them.*	*Apply critical thinking skills to evaluate potential risks and vulnerabilities related to cybercrimes against property in different scenarios.*	*Compare and contrast the UN Convention Against Transnational Organized Crime (2000) with other international instruments relevant to combating cybercrime, such as the Budapest Convention.*

SLO-8	*Distinguish between criminality and criminal liability in the context of cybercrimes, and apply relevant legal principles.*	*Define cyber terrorism, including its key ingredients, typical targets, and underlying motivations for engaging in this form of criminal activity.*	*Evaluate the potential financial and personal losses resulting from cyber fraud and cybertheft, and learn how to protect oneself from becoming a victim.*	*Develop strategies for preventing and mitigating cybercrimes against property through best practices and security measures.*	*Apply principles of international children's rights as enshrined in the Convention on the Rights of the Child (1989) and its optional protocols to cases involving child victims of cybercrime.*
SLO-9	*Apply the concepts of actus reus (guilty act) and mens rea (guilty mind) to specific cybercrimes.*	*Evaluate the role of hacktivism as a form of political protest or social activism, compared to more destructive forms of cyber terrorism.*	*Understand the dangers of installing spyware and other malicious software on one's devices, and explore methods for detecting and removing such threats.*	*Investigate and analyze evidence related to cybercrimes against property using appropriate tools and techniques.*	*Interpret the relevance of the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007) to issues surrounding sexual exploitation and abuse of minors online.*
SLO-10	*Tutorial: Challenges in the Deterritorialization in Cybercrimes*	*Tutorial: Seminar on the Impact of DDoS (Distributed Denial-of-Service) on a State's economy and public order.*	*Tutorial: Expert Talk on Cyber Fraud and their Prevention.*	*Tutorial: Group Discussion on the Incidence of Phishing in India.*	*Tutorial: Seminar on the Rising Incidence of Crimes against Children online*
SLO-11	*Practice: Pick any two Supreme Court or High Court cases involving appeals against cybercrime charges; and highlight the complexities in ascertaining mens rea and actus reus*	*Practice: Prepare a Differentiation Table showing the major differences between cyber warfare and cyber terrorism on the basis of at least the following criteria: Primary goals of the attack(s), Nature of the Actors involved, Legal framework and international norms, and the Key tactics and techniques used to carry out their attack(s).*	*Practice: Joining hands with the Clinical Legal Education Cell, draft a presentation or infographic on the Prevention of Cyber Fraud and Cyber Theft from electronic devices, and visit a certain number of schools nearby to sensitize students regarding this topic.*	*Practice: Analyze a problem scenario where an organization has been attacked by a ransomware attack that has encrypted all of its files and is demanding a large sum of money for their release. Identify potential risks and vulnerabilities that may have contributed to this attack, such as outdated software or lack of employee training on phishing emails, and suggest risk mitigation measures.*	*Practice: Analyze the definition of sexual abuse under Article 18 of the Council of Europe Convention on the Protection of children against sexual exploitation and sexual abuse (2007).*
SLO-12	*Practice: Summarize the Article titled 'Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts' by Cedric Ryngaert, https://doi.org/10.1017/glj.2023.24.*	*Practice: Write a short note on the concept of hacktivism and what are their common modus operandi.*	*Practice: Research on some of the most common and effective antivirus programs in both paid and free options.*	*Practice: Draft a password management policy for your organization, considering factors like automatic strong password generation and two-factor authentication.*	*Practice: Write a brief note on the principles imbibed under the Convention on the Rights of the Child, 1989 which aim at protecting children from sexual exploitation, and how they seek to prevent cybercrimes against children.*

SLO-13	*Assess the application of strict liability in cases of cybercrime, and evaluate its advantages and disadvantages.*	*Identify and explain different types of malicious software (malware), including viruses, worms, Trojan horses, and spyware.*	*Investigate the techniques used by spammers and email bombers to overwhelm individuals and organizations with unwanted messages, and discuss ways to mitigate their effects.*	*Evaluate the effectiveness of current laws and policies aimed at deterring and punishing cybercrimes against property.*	*Examine the legal framework governing cyber operations under the Tallinn Manual 2.0 International Law Applicable to Cyber Operations (2017), particularly in relation to state sovereignty and use of force.*
SLO-14	*Compare and contrast different types of cybercrimes, including those against property, individuals, reputation, and the state.*	*Describe best practices for implementing technical security measures to prevent or mitigate the effects of cyber threats, such as firewalls, intrusion detection systems, and encryption technologies.*	*Examine the harms caused by online voyeurism, child pornography, and other forms of sexual exploitation, and consider the role of law enforcement and technology companies in combating these crimes.*	*Understanding complex ideas and concepts related to cybercrimes against property effectively.*	*Demonstrate knowledge of India's national laws relating to cybercrime, such as the Information Technology Act, 2000 and amendments thereto, and their intersection with the IPC.*
SLO-15	*Investigate the involvement of transnational organized groups in cybercrimes, and analyze their impact on national and international security.*	*Assess the current laws and regulations designed to combat cyber terrorism, evaluating their effectiveness and identifying areas where further reform may be necessary.*	*Reflect on the challenges and opportunities presented by social media platforms, and develop responsible and safe practices for using them to communicate and share information.*	*Understand the ethical implications of engaging in or failing to prevent cybercrimes against property and develop a personal code of ethics regarding online behavior.*	*Critique current legal regimes and propose potential reforms to better address emerging challenges posed by cybercrime while balancing individual privacy and security concerns.*
SLO-16	*Tutorial: Changing Landscape of Strict Liability in Cybercrimes - the Doctrine of Abnormally Dangerous Activities*	*Tutorial: Seminar on some of the most dangerous viruses ever, and how they impacted users on the internet.*	*Tutorial: Seminar on Managing spam and inappropriate content on social media*	*Tutorial: Group Discussion on the rise of phishing scams in India.*	*Tutorial: Group Discussion on new Emerging Cybercrimes in India and beyond.*
SLO-17	*Practice: Scour the internet to observe 10 websites where objectionable content has been posted/aired/featured. Write a short note on the various types of cybercrimes that may be attracted by these objectionable content.*	*Practice: Create a secure communication channel between two endpoints (e.g., client and server), using OpenSSL or any other tools.*	*Practice: Analyzing Spamming and Email Bombing Techniques done by Websites and other Online Services, by setting up an email account specifically for this exercise, and then subscribing to various newsletters, free trials, and promotional offers.*	*Practice: Identify a specific type of cybercrime against property that you believe is particularly difficult to detect or prosecute, botnet attacks pr phishing attacks, and analyze whether the existing laws and policies aimed at preventing and punishing this type of crime are effective.*	*Practice: Based upon the above Group Discussion, write a Report on what reforms and amendments are needed to strengthen protection of liveware against cybercrimes.*

SLO-18	*Practice: Analyze whether internet platforms should be held strictly liable for objectionable content posted on their platforms.*	*Practice: Examine the National Cyber Security Policy, 2013, released by the Department of Electronics and Information Technology (DeitY), and critique this Policy.*	*Practice: Based on the analysis in the above exercise, implement relevant anti-spam measures and tools on the dedicated email account, such as ad-blockers, filters, blocklists, challenge-response systems, or other third-party software, and comment on the changes brought in terms of how spamming has reduced.*	*Practice: Research 1 Indian and 1 foreign judgment each deciding on any specific type of cybercrime against property, compare the ratio decidendis applied by the Courts in the two cases, and comment on how different the jurisprudence pertaining to that cybercrime is in India as compared to the other's.*	*Practice: Write a short note on the principle of neutrality in cyber operations under the Tallinn Manual 2.0 International Law Applicable to Cyber Operations (2017).*

Assessment	*Continuous Learning Assessment - 1*	*Continuous Learning Assessment - 2*
	Continuous Learning Assessment - 3	

Resources			
1	S.V. Joga Rao, Law of Cyber Crime and Information Technology, Wadhwa and Co., Nagpur.	2	Paul Cornish, The Oxford Handbook of Cyber Security, OUP 2021.
3	R. C Mishra, Cyber Crime Impact in the New Millennium, Auther Press. Edition 2010.	4	Barkha and U. Ram Mohan, Cyber Law s and Crimes, 3rd Edit ion, Delhi Law House.
5	Babak Akhgar & Andrew Staniforth & Francesca Bosco, Cyber Crime and Cyber Terrorism Investigator's Handbook (2014).	6	Andrew Murray, The Regulation of Cyberspace, 2006; Rutledge – Cavendish.
7	Ian Walden, Computer Crimes and Digital Investigations, OUP 2016.	8	Peter Grabosky, Henry N. Pontell, Cyber Crime, OUP 2015.
9	Jens David Ohlin, Kevin Govern, Claire Finkelstein, Cyber War, OUP 2015.	10	Andrew Murray, Information Technology Law, OUP 2023.

Rationale (CLR)	*The purpose of learning this course is to:*	Depth				Attainment			Program Learning Outcomes (PLO)												
		1	2	3	4	1	2	3	1	2	3	4	5	6	7	8	9	10	11	12
CLR-1	*Define the concept of cybercrime and its significance in modern society, and understand the different types of cyber crimes and their impact on individuals, businesses, and governments.*																			
CLR-2	*Analyze the legal and ethical considerations involved in creating new laws to address cybercrime, and evaluate the potential unintended consequences of over-criminalization or under-criminalization of activities in cyberspace.*																			
CLR-3	*Learn the elements required for a behavior to be considered a cybercrime; distinguishing between different types of cyber crimes based on their level of sophistication and organization, along with the motivations behind different forms of cybercrime, such as financial gain, political activism, or personal revenge, etc.*																			
CLR-4	*Understanding the various approaches to attribution and responsibility in cyberspace, along with the application of actus reus and mens rea to specific cybercrime scenarios, considering the role of strict liability and other principles of criminal liability in specific cybercrimes.*																			
CLR-5	*Learning the various types of cybercrimes according to their targets (property, individuals, reputation, or state), assessing the implications of transnational organized crime for law enforcement and international cooperation, and the appropriate responses to cyber threats at the national and global levels, including diplomatic, economic, and military measures.*																			

Outcomes (CLO)	*At the end of this course, learners will be able to:*	Conceive	Design	Implement	Operate	Level of Thinking	Expected Proficiency (%)	Expected Attainment (%)	Disciplinary Knowledge	Critical Thinking	Problem Solving	Analytical Reasoning	Research-related Skills	Communication Skills	Cooperation/Team Work	Digital Literacy	Self-directed Learning	Moral and Ethical Reasoning	Leadership Qualities	Life Long Learning
CLO-1	*Understand the concept of crime in cyberspace, definitions of cybercrime and its criminalization in different jurisdictions; behavior exhibited in cybercrimes and the legal requirements necessary to establish criminality and liability including jurisdiction and classification of cybercrimes, based on the victim(s), such as crimes against property, individuals, reputation, and states.*	☐	☐		-	*2*	*85*	*75*	*3*	*2*	-	*1*	-	*3*	-	*2*	*2*	*1*	*2*	*3*
CLO-2	*Learn the nature of cyberwarfare and cyberterrorism, including their defining characteristics, ingredients, targets, motivations, and offenders; along with analyzing technical security measures that combat cyberterrorism and other similar threats.*	☐	☐	☐	-	*2*	*85*	*75*	*3*	*2*	*1*	*2*	*2*	*3*	*2*	*1*	*2*	*1*	*2*	*3*
CLO-3	*Learn the various cybercrimes targeted at individuals, such as cyberbullying, cyberstalking, identity theft, phishing, cyber fraud, voyeurism, social media frauds, online drug trafficking, etc., and groups of individuals, such as cybercrimes against women and transgenders.*	☐	☐	☐	☐	*3*	*85*	*75*	*3*	*1*	*3*	*1*	*3*	*3*	-	*1*	*1*	*2*	*1*	*3*
CLO-4	*Investigate various cybercrimes related to property, such as computer trespassing, dissemination of viruses, hacking networks, website access by unauthorized parties, intellectual property crimes, credit card fraud, disk loading, internet time theft, and cybersquatting.*	☐	☐	☐	☐	*3*	*85*	*75*	*3*	*3*	*2*	*3*	*3*	*3*	*2*	*2*	*3*	*3*	*3*	*3*
CLO-5	*Review major international and national laws established to combat cybercrime, such as the Budapest Convention, Palermo Convention, Tallinn Manual, IT Act, and IPC. Familiarizing themselves with these conventions and statutes, enabling learners to appreciate how Governments worldwide address these challenges through legislation and cooperation.*	☐	☐	☐	☐	*3*	*85*	*75*	*3*	*3*	*2*	*3*	*3*	*3*	*1*	*3*	*3*	*3*	*3*	*3*

Assessment Method (Max. Marks: 100)													
		Continuous Learning Assessment (CLA 40% Weightage)								Final Exam	
Level of Thinking		Model Exam (20%)		Assignment/ Seminar/Group discussion/ Presentation		Participation in seminar/ Conference/ Publication		Participation in class room/co-curricular & Para curricular activities			
		(20%)		(10%)		(5%)		(5%)		(60%)	
1	Remember	40%	-	40%	-	30%	-		-	40%	-
2	Understand										
3	Apply	40%	-	40%	-	40%	-		-	40%	-
4	Analyze										
5	Evaluate	20%	-	20%	-	30%	-		-	20%	-
6	Create										
Total		100 %		100 %		100 %		100 %		100 %	

Strategies					
Technology		Pedagogy / Andragogy		Sustainable Development	
Simulations	☐	Clarification/Pauses	☐	Good Health & Well Being	☐
Presentation Tools	☐				
Learning Management System		Group Discussion	☐	Quality Education	☐
		Hands-on Practice	☐		
		Debate	☐		
		Interactive Lecture	☐		
		Brainstorming	☐		

Designers					
Professional Experts		Higher Institution Experts		Internal Experts	
1	*<name>, <industry name>, <email id>*	1	*<name>, <institution name>, <email id>*	1	*Prof.(Dr) Revvathy Venkaraman, FSH faculty, SRMIST*
2	*<name>, <industry name>, <email id>*	2	*<name>, <institution name>, <email id>*	2	*<name>, SRMIST, <email id>*

Code	PLCS24203T	Title	CONSTITUTIONAL AND LEGAL ASPECTS OF CYBER SPACE & INTERNET	Category		Professional Core	L	T	P	C
							3	1	2	5

Course Offering Department	School of Law	Pre-requisite Courses		Co-requisite Courses		Progressive Courses		Data Book / Codes/Standards	

Title & Content	Unit 1	Unit 2	Unit 3	Unit 4	Unit 5
Duration (hour)	18	18	18	18	18
SLO-1	*Define and explain the concept of constitutionalism in the context of digital governance.*	*Explain the concept of human rights in relation to the internet and understand why they are essential in protecting individuals' freedom online.*	*Explain the principle of state sovereignty in the context of cyberspace, including the rights and duties it entails for states and other actors.*	*Explain the importance of applying constitutional principles consistently across different technologies, including cyberspace.*	*Distinguish cyber law from other areas of law, including its unique features and challenges.*
SLO-2	*Analyze the implications of digital sovereignty for modern states and their citizens.*	*Analyze the principles outlined in the IRPC charter that aims at ensuring human rights protection in the digital age.*	*Analyze the application of the non-intervention principle to cyber operations, identifying situations where intervention may be considered a violation of international law.*	*Learn about digital constitutionalism and describe its key components.*	*Explain the concept of territoriality and how it applies to cyberspace, identifying both its benefits and limitations in regulating online conduct.*
SLO-3	*Identify and evaluate the challenges posed by the hybridization of public and private functionaries in the digital age.*	*Evaluate the significance of the Charter of Human Rights and Principles for the Internet, 2023, and its impact on preserving internet rights.*	*Apply the due diligence standard to cyber incidents, evaluating whether a state has fulfilled its obligation to prevent harm caused by private actors within its jurisdiction.*	*Analyze the distinctions between public and private actors in regulating speech, expression, privacy, and other social values online.*	*Analyze the role of states in regulating cyberspace conduct, recognizing their sovereign authority while also acknowledging the limits of their power due to jurisdictional issues and the transnational nature of cyberspace.*

SLO-4	*Tutorial: Group Discussion on the Current Status of Freedom of Expression in India in cyberspace.*	*Tutorial: Seminar on the international human rights that are applicable to free speech in cyberspace.*	*Tutorial: Seminar on the Interplay between International Law and Cyberspace.*	*Tutorial: Seminar on how Facial Recognition Software can affect Human Rights*	*Tutorial: Seminar on the Changing Landscape of Cyber law, and the Issues and Challenges that lie ahead.*
SLO-5	*Practice: Choose any country and research its approach to digital sovereignty. Consider factors such as national security, economic growth, and civil liberties. Compare them with those of India.*	*Practice: Prepare a presentation highlighting any discrepancies between India's legal framework and the IRPC Charter of Human Rights and Principles for the Internet, 2023.*	*Practice: Problem Question relating to how a tech company headquartered in Country A but operates servers and data centers in various countries around the world, including Country B, is forced by the Government of Country B to hand over access to user data stored on these servers claiming that data has been stored without proper legal procedures or international agreements, thereby alleging violation of national laws.*	*Practice: Debate on two scenarios involving potential regulation of speech, expression, privacy, or other social values online. In the first scenario, the subject is a government entity; in the second scenario, the subject is a private company.*	*Practice: Choose any real-life problem scenario and analyze the substantial and procedural legal aspects in the implementation and enforcement of the law and access to justice.*
SLO-6	*Practice: Suppose the student is a policymaker tasked with regulating the use of facial recognition technology by law enforcement. Develop a simple framework for balancing the interests of public safety and individual privacy, taking into account the role of private companies that develop and sell facial recognition software.*	*Practice:* *Brief Write-up on the UN General Assembly Resolution on "The right to privacy in the digital age" (A/RES/68/167)*	*Practice: Brief Write-up of the Conflict between National Security and State Sovereignty in Cyberspace.*	*Practice: Analyze 3 cases where digital constitutionalism has been applied or discussed.*	*Practice: Analyze a problem scenario where the potential conflicts arising from differing national regulations and possible solutions*

SLO-7	*Understand and assess the ways in which traditional notions of rights and freedoms are being fragmented in the digital era.*	*Compare and contrast different theories related to cyberspace, including cyberspace exceptionalism theory, and assess their implications for internet governance and regulation.*	*Evaluate the responsibility of states for internationally wrongful acts committed in cyberspace, considering issues of attribution and countermeasures.*	*Apply the concept of "constitutional morality" to evaluate state actions affecting civil liberties in cyberspace.*	*Identify different legal frameworks that govern various aspects of cyberspace conduct, such as criminal law, tort law, intellectual property law, contract law, data protection law, and privacy law.*
SLO-8	*Critically examine instances of over-interference into individual rights and freedoms in the name of national security or public order.*	*Identify various forms of virtual realities and describe how these technologies can affect users' perceptions and experiences of the world.*	*Compare and contrast the role of international human rights law and international humanitarian law in regulating cyber operations during peacetime and wartime.*	*Evaluate the roles of public policy and private policy in shaping behavior and protecting rights in cyberspace.*	*Compare and contrast key provisions of major cyber-related legislation, including the Information Technology Act, 2000, the Bharatiya Nyaya (Second) Sanhita, 2023, the Digital Personal Data Protection (DPDP) Act, 2023, the Copyright Act, 1957, the Trade Marks Act, 1999, and others.*
SLO-9	*Articulate the constitutional boundaries of digital sovereignty and their impact on individual privacy and autonomy.*	*Recognize potential threats associated with internet usage such as physical harm, social issues, and addiction, and propose strategies for addressing them effectively.*	*Assess the legality of cyber threats and uses of force under international law, applying concepts such as necessity, proportionality, and self-defense.*	*Compare and contrast constitutional norms and private regulatory mechanisms for governing online activities.*	*Evaluate the effectiveness of specific rules and regulations governing electronic service delivery, intermediary liability, digital media ethics code, guidelines for cyber cafes, and incident response procedures in promoting security and protecting user rights.*
SLO-10	*Tutorial: How social media platforms can limit free expression through terms of service policies.*	*Tutorial: Delve into the world of Virtual Reality and examine how the Rights of persons may be affected in VR scenarios.*	*Tutorial: Seminar/Discussion on the Scope & Extent of Tortious Principles of State Responsibility in Cyberspace.*	*Tutorial: Seminar on Constitutional Morality vs. Public Morality in Cyberspace*	*Tutorial: Seminar on how cybercrimes are dealt with under the Bharatiya Nyaya (Second) Sanhita, 2023.*

SLO-11	*Practice: Identify three recent cases where governments have allegedly interfered excessively with individuals' rights and freedoms in the name of national security or public order.*	*Practice: Summarize the Article titled 'Regulating Cyberspace: An Examination of Three Theories' by Dr. Bernard Oluwafemi Jemilohun, International Journal of Business and Management Invention (IJBMI) ISSN (Online): 2319 – 8028, ISSN (Print): 2319 – 801X, www.ijbmi.org, Volume 8 Issue 05 Series. I, (2019). pp. 20-26.*	*Practice: Analyze how international human rights law applies to a situation where a nation has implemented strict internet surveillance measures to monitor extremist activities online within its borders, with criticisms that these measures may infringe upon citizens' freedom of expression and privacy rights.*	*Practice: Analyse a problem scenario involving tension between constitutional norms and private regulatory mechanisms.*	*Practice: Compare and contrast the interpretations of "cybercrime" or like terms under the Information Technology Act, 2000, the Bharatiya Nyaya (Second) Sanhita, 2023.*
SLO-12	*Practice: Essay on how interference in fundamental rights may be necessary for maintaining public order in cyberspace.*	*Practice: Analyze a problem case scenario of sexual harassment on any popular VR platform, and what legal measures may be available for pursuit of justice.*	*Practice: Analyze an international humanitarian law scenario where one State decides to launch a cyber-operation targeting an enemy State's military communication systems, and causing collateral damage to civilian's computer systems.*	*Practice: Compare and contrast Government regulations & corporate rules and guidelines, for preventing hate speech.*	*Practice: Pick any two legislations studied in this unit, and assess whether there are any inconsistencies or overlapping of legal provisions.*
SLO-13	*Navigate the complex legal landscape surrounding freedom of speech and expression in the social media era.*	*Understand the importance of free speech and access to information as fundamental human rights, and evaluate ways to address challenges like internet censorship and cyberbullying.*	*Describe the mechanisms available for the peaceful settlement of cyber-related disputes, analyzing their strengths and weaknesses.*	*Describe the relationship between the rule of law and cyberspace, particularly as it relates to limiting governmental power and promoting accountability.*	*Apply legal principles to real-world scenarios involving cyber crimes, breaches of confidential information, infringement of intellectual property rights, violations of contracts, unauthorized access, and invasion of privacy.*

SLO-14	*Apply principles of reasonableness and proportionality when evaluating potential limits on free speech and other fundamental rights.*	*Examine international legal instruments that protect human rights, such as the Universal Declaration on Human Rights of 1948, and apply this knowledge to current debates surrounding internet governance and policy-making.*	*Identify the challenges posed by cyber activities to international peace and security, proposing strategies for addressing them through multilateral cooperation and collective security arrangements.*	*Assess the impact of discrimination, hate speech, and protests on individual rights and societal values in virtual spaces.*	*Synthesize legal arguments based on relevant statutes, cases, and ethical considerations when advising clients, drafting documents, negotiating agreements, or litigating disputes related to cyber activities.*
SLO-15	*Engage in thoughtful deliberation about how to balance state power with individual freedom in an increasingly interconnected world.*	*Critically reflect upon the complex relationship between technology and society, recognizing both the opportunities and risks presented by the rapidly evolving digital landscape.*	*Formulate recommendations for the development of international telecommunications law that takes into account the unique characteristics of cyberspace while ensuring respect for fundamental human rights and principles of international law.*	*Critique the substantive and procedural limitations on free speech in cyberspace, including legal precedents set by courts and contributions made by judges to develop a body of case law around these issues.*	*Reflect on emerging trends and future developments in cyber law, considering factors like technological innovation, globalization, evolving social norms, and changing regulatory approaches.*
SLO-16	*Tutorial: Seminar on Balancing State Power and Individual Freedom Through Policy Development.*	*Tutorial: Group Discussion on cyberbullying and its impact on victims' mental health.*	*Tutorial: Seminar on the Role of International Institutions like the Permanent Court of Arbitration (PCA), International Chamber of Commerce (ICC), or United Nations Commission on International Trade Law (UNCITRAL) in resolving international cyber-related disputes.*	*Tutorial: Seminar on the Necessity of Observing Principles of the Rule of Law such as transparency, consistency, and accountability in Cyberspace regulation.*	*Tutorial: Group Discussion on How Globalization has led to the Growth of Cyber Laws.*

SLO-17	*Practice: A brief write-up on how the principle of proportionality is necessary in the enforcement of cyber law.*	*Practice: Brief Write-up on Right to Access Internet as a Fundamental Right*	*Practice: Research any one existing mechanism for the peaceful resolution of cyber-related disputes, and analyze its efficacy.*	*Practice: Assess how rule of law is affected in a situation where the Government has attempted to regulate online activity or limit access to information which criticizes the Government.*	*Practice: A hypothetical bank has been reported to be the victim of a sophisticated cyber attack resulting in the theft of lakhs of customers' personal identification information (PII). The bank suspects that an international hacking group is behind the attack. Analyze the potential criminal charges that could be brought against the perpetrators under Indian and international laws, as well as any jurisdictional issues that may arise.*
SLO-18	*Practice: Identify 3 recent instances of accounts being banned on Twitter (X) or YouTube, and whether those grounds were justified.*	*Practice: Identify 3 recent instances of internet blockades and comment on whether they were justified.*	*Practice: Advise a Government agency by way of a policy brief as to how it can defend/justify a sensitive data breach of a foreign company.*	*Practice: Analyze the Strengths and Weaknesses of using Virtual Spaces for Activism.*	*Practice: Analyze the cyber legal aspects in the US case of Stardock Systems, Inc. v. Paul Reiche III and Robert Frederick Ford, 2018 WL 7348858 (N.D. Cal. 2018); what are the takeaways from this case?*
Assessment	*Continuous Learning Assessment - 1*		*Continuous Learning Assessment - 2*		
	Continuous Learning Assessment - 3				

Resources			
1	Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd.	2	Edoardo Celeste, Digital Constitutionalism, Routledge, 2022.
3	Kriangsak Kittichaisaree, Public International Law of Cyberspace, Springer Link, 2017.	4	Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd.
5	Data Privacy Principles and Practice by Natraj Venkataramanan and Ashwin Shriram, CRC Press.	6	Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers.
7	Information Security Governance, Guidance for Information Security Managers by W. KragBrothy, 1st Edition, Wiley Publication.	8	Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform. (Pearson , 13th November, 20xs01)
9	Law on Information Technology by Ishita Chatterjee, 3rd Edition, 2022.	10	M Mueller, Will the Internet Fragment? Sovereignty, Globalization and Cyberspace (Polity Press 2017).

Rationale (CLR)	*The purpose of learning this course is to:*	Depth				Attainment			Program Learning Outcomes (PLO)											
CLR-1	*Familiarize Students with key organizations like the IRPC, which advocate for human rights in the digital sphere. They will also study the Charter of Human Rights and Principles for the Internet (2023), gaining insight into how these fundamental protections translate into the virtual domain.*	1	2	3	4	1	2	3	1	2	3	4	5	6	7	8	9	10	11	12
CLR-2	*Explore the diverse forms of virtual reality environments, including simulated worlds and augmented experiences, students will identify potential risks linked to each type. From physical dangers like cyberstalking to psychological consequences stemming from internet addiction, this module aims to raise awareness regarding the need for robust safeguards*	*Conceive*	*Design*	*Implement*	*Operate*	*Level of Thinking*	*Expected Proficiency (%)*	*Expected Attainment (%)*	*Disciplinary Knowledge*	*Critical Thinking*	*Problem Solving*	*Analytical Reasoning*	*Research-related Skills*	*Communication Skills*	*Cooperation/Team Work*	*Digital Literacy*	*Self-directed Learning*	*Moral and Ethical Reasoning*	*Leadership Qualities*	*Life Long Learning*
CLR-3	*Focus specifically on issues related to freedom of expression, students will discuss problems associated with internet censorship, cyberbullying, and various forms of hate speech. Drawing from existing international treaties and conventions, they will investigate possible countermeasures aimed at promoting inclusivity and protecting vulnerable communities.*																			
CLR-4	*Grapple with dilemmatic questions pertaining to striking a balance between individual liberties and broader communal goals. For instance, what are the acceptable limits on freedom of expression when faced with harmful rhetoric or incitement? How can states reconcile competing demands while upholding core human rights tenets?*																			
CLR-5	*Apply Legal Standards Across Jurisdictions: Lastly, students will compare and contrast approaches taken by different countries vis-à-vis implementing human rights standards in cyberspace. Using comparative analysis techniques, they will evaluate strengths and weaknesses inherent in various national strategies and propose improvements based on best practices gleaned globally.*																			
Outcomes (CLO)	*At the end of this course, learners will be able to:*																			
CLO-1	*Define and explain the concept of digital sovereignty and how it relates to constitutionalism in the digital age, and Evaluate the scope and extent of freedom of speech and expression in the social media era and understand the limitations of reasonable restrictions.*				-	2	85	75	3	-	2	1	-	3	-	2	2	1	2	3
CLO-2	*Explain the relationship between the Internet Rights and Principles Dynamic Coalition (IRPC), the Charter of Human Rights and Principles for the Internet, and internet rights, and the various threats associated with internet usage, including physical, social, and psychological risks.*				-	2	85	75	3	2	1	2	2	3	-	1	2	1	2	3
CLO-3	*Apply relevant legal frameworks to specific scenarios involving cyber attacks and analyze their legality, assessing the applicability of international human rights law in cyber space and its intersection with international humanitarian law.*					3	85	75	3	1	3	1	3	3	-	1	1	2	1	3
CLO-4	*Analyze the regulatory landscape surrounding speech, expression, privacy, and social values in both public and private domains, and Understand the interplay between rule of law, governance, and discrimination, and apply legal reasoning to resolve conflicts arising from competing interests.*					3	85	75	3	3	2	3	3	3	-	2	3	3	3	3
CLO-5	*Distinguish between different legal frameworks applicable to cyber space, including criminal law, tort law, IP law, contract law, data protection law, and privacy law, and Analyze the strengths and weaknesses of various legislative instruments used to regulate cyber space.*					3	85	75	3	3	2	3	3	3	-	3	3	3	3	3

Assessment Method (Max. Marks: 100)													
		Continuous Learning Assessment (CLA 40% Weightage)								Final Exam	
Level of Thinking		Model Exam (20%)		Assignment/ Seminar/Group discussion/ Presentation		Participation in seminar/ Conference/ Publication		Participation in class room/co-curricular & Para curricular activities			
		(20%)		(10%)		(5%)		(5%)		(60%)	
1	Remember	40%	-	40%	-	30%	-		-	40%	-
2	Understand										
3	Apply	40%	-	40%	-	40%	-		-	40%	-
4	Analyze										
5	Evaluate	20%	-	20%	-	30%	-		-	20%	-
6	Create										
Total		100 %		100 %		100 %		100 %		100 %	

Strategies					
Technology		Pedagogy / Andragogy		Sustainable Development	
Simulations		Clarification/Pauses		Good Health & Well Being	
Presentation Tools					
Learning Management System		Group Discussion		Quality Education	
		Hands-on Practice			
		Debate			
		Interactive Lecture			
		Brainstorming			

Designers					
Professional Experts		Higher Institution Experts		Internal Experts	
1	*<name>, <industry name>, <email id>*	1	*<name>, <institution name>, <email id>*	1	*<name>, SRMIST, <email id>*
2	*<name>, <industry name>, <email id>*	2	*<name>, <institution name>, <email id>*	2	*<name>, SRMIST, <email id>*

Code	PLCS24204T	Title	INTERNATIONAL & NATIONAL PERSPECTIVE OF CYBER LAW	Category		Professional Core	L	T	P	C
							3	1	2	5

Course Offering Department	School of Law	Pre-requisite Courses		Co-requisite Courses		Progressive Courses		Data Book / Codes/Standards	

Title & Content	Unit 1	Unit 2	Unit 3	Unit 4	Unit 5
Duration (hour)	18	18	18	18	18
SLO-1	*Understand the key organizations involved in international governance of the internet, including IETF, ISOC, ICANN, ITU, IGF, OECD, CIGI, and CDT, and their respective roles and responsibilities.*	*Understand the key principles and concepts of governance of e-commerce resources, including the management and allocation of Internet domains and other digital assets.*	*Understand the importance of safeguarding privacy and personal data protection in the context of human rights and international law.*	*Describe the key provisions and goals of the United Nations Convention Against Transnational Organized Crime (2000), including its relevance to combating cybercrime, cyber warfare, and cyberterrorism.*	*Understand the role of national governance in shaping information technology policies and regulations in India.*
SLO-2	*Explain the importance of technical standards in ensuring interoperability and functionality of the internet, and describe the role of the IETF in developing these standards.*	*Analyze the significance of the Convention on the Use of Electronic Communications in International Commerce (2005), including its role in promoting trust and certainty in cross-border electronic transactions.*	*Explain the key provisions and requirements of the major Council of Europe treaties related to data protection, including the Convention for Protection of Individuals with Regard to Automatic Processing of Personal Data (1981), the Additional Protocol to the Convention regarding supervisory authorities and transborder data flows (2001), and the Protocol amending the Convention (2018).*	*Analyze the main features of the Convention on Cybercrime (2001), also known as the Budapest Convention, such as its scope, objectives, and mechanisms for international cooperation in investigations and prosecutions.*	*Analyze the key provisions and impact of the Information Technology Act 2000 (IT Act 2000) and its amendments on cybercrime prevention and digital evidence collection in India.*

SLO-3	*Analyze the relationship between the various bodies responsible for internet governance, such as IESG, IAB, and W3C, and understand how they collaborate to ensure a unified approach to internet architecture and design.*	*Compare and contrast the provisions of the UNCITRAL Model Law on Electronic Commerce (1996) with those of national laws governing e-commerce, identifying areas of convergence and divergence.*	*Analyze how the UN Human Rights instruments, such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (1966), address issues related to privacy and data protection.*	*Compare and contrast the content of the Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist or Xenophobic Nature Committed Through Computer Systems (2003) with that of the original convention.*	*Evaluate the significance of the IT Act's recognition of electronic records and digital signatures as legally valid forms of communication and authentication.*
SLO-4	*Tutorial: Group Discussion on how the above mentioned organizations ensure the smooth functioning of the internet.*	*Tutorial: Discuss how far the above mentioned international conventions have been incorporated into Indian Law.*	*Tutorial: Seminar on How Big data enables flow of personal data across frontiers by automatic processing, causing violation of privacy.*	*Tutorial: Seminar on Recent Global Cyber Attacks and how they Impact the Economy of Affected Nations*	*Tutorial: Discussion on the incidence of cybercrimes in India under the IT Act, 2000 as per the latest available National Crime Records Bureau (NCRB) Reports.*
SLO-5	*Practice: Article Summary - OECD (2012-11-16), "The Role of the 2002 Security Guidelines: Towards Cybersecurity for an Open and Interconnected Economy", OECD Digital Economy Papers, No. 209, OECD Publishing, Paris. http://dx.doi.org/10.1787/5k8zq930xr5j-en.*	*Practice: Brief Write-Up on the Salient Features of the UNCITRAL Model Law on Electronic Commerce (1996).*	*Practice: Analyze the nature of the right to obtain information stored as automated personal data file under the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981.*	*Practice: Identify the key provisions and goals of the Convention Against Transnational Organized Crime (2000), paying particular attention to Articles 5-9, which deal with criminalization, liability of legal persons, jurisdiction, and mutual legal assistance.*	*Practice: Brief Write-Up on Assessing the Impact of the IT Act 2000 and Its Amendments on Cybercrime Prevention and Digital Evidence Collection*
SLO-6	*Practice: Read the Web Content Accessibility Guidelines (WCAG) 2.0 and examine what all guidelines are relevant in terms of law.*	*Practice: Write an Essay on the Legality of Electronic Data Messages in Contractual Formation from an Indian Context.*	*Practice: Perform an ILAC Analysis on the case Riley v. Student Housing Co (Ops) Ltd [2023] 2 WLUK 278 in the context of ascertaining the extent to which disclosure of personal data is permissible*	*Practice: Practice: Enumerate and summarize 5 judicial precedents in the past decade involving a charge of offences involving racist or xenophobic nature committed through computer systems.*	*Practice: Examine the changes brought about by the IT (Amendment) Act 2008, particularly those related to the admissibility of digital evidence in court proceedings under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023.*

SLO-7	*Describe the process by which domain names are managed and assigned through ICANN and its bylaws, and explain the significance of the UDRP in resolving disputes over domain name ownership.*	*Evaluate the impact of the Model Law on Electronic Signatures (2001) on the legal recognition and admissibility of electronic signatures in different jurisdictions.*	*Compare and contrast the GDPR's approach to protecting individuals' personal data with that of other relevant legal frameworks, such as the Council of Europe treaties and the UN Human Rights instruments.*	*Evaluate the significance of the Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence (2022) in addressing challenges posed by modern information technologies to criminal justice systems.*	*Explain the importance of data protection and privacy in the context of India's digital economy, including an understanding of the principles underlying the Digital Personal Data Protection Act 2023.*
SLO-8	*Evaluate the impact of international telecommunications regulations on internet governance, with reference to the work of the ITU and other relevant organizations.*	*Apply the provisions of the Model Law on Electronic Transferable Records (2017) to specific scenarios involving the use of electronic records in commercial transactions.*	*Apply best practices and strategies for implementing effective data protection measures within organizations, taking into account applicable laws and regulations.*	*Identify the major principles and standards set forth in the Convention on the Rights of the Child (1989) and their implications for protecting children's rights online.*	*Compare and contrast the data protection requirements under the IT Act and the DPDPA 2023, identifying areas where further clarification or reform may be needed.*
SLO-9	*Compare and contrast different approaches to internet governance at the national level, taking into account issues related to jurisdiction, sovereignty, and human rights.*	*Explain the mandate and activities of the Working Group on Online Dispute Resolution within the context of global e-commerce regulation.*	*Evaluate potential risks and vulnerabilities associated with collecting, storing, processing, sharing, and transferring personal data across borders.*	*Examine the role of the Optional Protocol to the Convention on the Rights of the Child (2001) in preventing the sale of children, child prostitution, and child pornography through cyberspace.*	*Describe the scope and objectives of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, including their implications for online intermediaries such as social media platforms and messaging apps.*
SLO-10	*Tutorial: Seminar on the Importance of ICANN with respect to Internet Protocol (IP) address space allocation, protocol parameter assignment, domain name system (DNS) management and root server system management.*	*Tutorial: Group Discussion on how digital signatures have ensured security and uniformity with respect to signing of documents online.*	*Tutorial: Debate on the topic "Free Data Flow is Paramount and must be Unhindered by Cybersecurity Concerns".*	*Tutorial: Seminar on the Principles and Standards Set Forth in the Convention on the Rights of the Child (2001).*	*Tutorial: Group Discussion or Debate on Whether the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 is Excessive Censorship which may potentially Gag social media.*

SLO-11	*Practice: Perform an ILAC analysis on possible real-world problem scenarios such as clash of domain names, etc.*	*Practice: Elucidate on the principles imbibed under the UNCITRAL Technical Notes on Online Dispute Resolution, 2017, with regards to facilitating fair and voluntary online dispute resolution.*	*Practice: Examine the Impact of GDPR on the protection of individuals' personal data.*	*Practice: Develop a tabletop exercise simulating a multinational law enforcement operation targeting an organized crime syndicate engaging in online activities related to the sale of children, child prostitution, or child pornography. Assign roles to participants, including law enforcement officers, prosecutors, policy makers, and representatives from NGOs working on child protection.*	*Practice: Identify 5 recent cases related to data breaches or misuse of personal information in India and analyze the impact it had on individuals and businesses involved in such breaches.*
SLO-12	*Practice: Comment on the working of the Uniform Domain-Name Dispute-Resolution Policy (UDRP).*	*Practice: Examine the issues concerning digital signatures in India.*	*Practice: Write a brief note on what are the most important principles for data protection.*	*Practice: Assign students different articles from the Convention on the Rights of the Child related to children's rights online (e.g., Articles 3, 13, 16, 17, 19). Instruct students to research real-world examples where these rights have been violated or upheld online.*	*Practice: Brief write-up on the key principles of the Digital Personal Data Protection Act 2023 (DPDPA), such as consent, purpose limitation, data minimization, etc.*
SLO-13	*Explore the role of civil society organizations like the Freedom Online Coalition in advocating for an open and accessible internet that respects human rights and promotes democratic values.*	*Assess the role of the World Intellectual Property Organization (WIPO) in protecting and enforcing intellectual property rights in the digital age.*	*Identify ethical considerations surrounding data collection, its storage, use, and dissemination, and develop appropriate guidelines for addressing them.*	*Summarize the core elements of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007) and assess its effectiveness in tackling sexual abuse committed via digital means.*	*Critically assess the balance between freedom of expression and content moderation under the Intermediary Guidelines and Ethics Code, particularly with respect to issues such as fake news and hate speech.*

SLO-14	*Examine the challenges posed by emerging technologies and applications, such as artificial intelligence and blockchain, to existing models of internet governance, and consider possible solutions to these challenges.*	*Compare and contrast the requirements of the Budapest Treaty on the International Recognition of the Deposit of Microorganisms for the Purposes of Patent Procedure with those of other international treaties governing patent protection.*	*Demonstrate an understanding of the role of oversight bodies, such as national data protection authorities and the European Data Protection Board, in enforcing compliance with data protection legislation.*	*Assess the value of the Tallinn Manual and primary law applicable to cyber conflicts in providing guidance for states when responding to malicious activities in cyberspace.*	*Identify the challenges and opportunities presented by emerging technologies such as artificial intelligence and blockchain in the Indian regulatory landscape, and consider how existing laws and frameworks might need to adapt.*
SLO-15	*Reflect on the broader implications of internet governance for global development, security, and social justice, and develop strategies for engaging with policymakers, industry leaders, and other stakeholders to promote a more inclusive and equitable digital future.*	*Critique the strengths and weaknesses of existing legal frameworks for regulating e-commerce and make recommendations for improvement based on current trends and developments in technology and business practices.*	*Develop strategies for resolving disputes related to data protection violations through diplomacy or alternative dispute resolution mechanisms.*	*Differentiate between the 1999 International Convention for the Suppression of the Financing of Terrorism and the 2005 International Convention for the Suppression of Acts of Nuclear Terrorism, particularly regarding their respective definitions of terrorist offenses and penalties.*	*Reflect on broader questions around the ethics of technological development and use in India, including issues of accessibility, affordability, and inclusivity, and the responsibilities of government, industry, and civil society actors in ensuring a just and equitable digital future.*
SLO-16	*Tutorial: Discussion on the Guiding Principles on Government Use of Surveillance Technologies (2023) by the Freedom Online Coalition*	*Tutorial: Seminar on how the two "Internet Treaties" administered by WIPO ensure that copyrights on the internet are protected.*	*Tutorial: Assessing Ethical Considerations and Regulatory Requirements for Storing and Maintaining Personal Data of Users*	*Tutorial: Seminar on the primary sources of international law relevant to cyber conflicts, such as treaties, customary international law, general principles, and judicial decisions.*	*Tutorial: Seminar on blockchain technology and whether it is actually making waves in a supposed 'unregulated' money market.*
SLO-17	*Practice: Project on the Role of Blockchain Management in Cybersecurity*	*Practice: Write a short note on how the Consumer Protection (E-Commerce) Rules, 2020 enhances cybersecurity on e-commerce platforms.*	*Practice: Critically Analyze the blog "Redefining Resolution in Data Disputes: Why Arbitration Holds the Key" by Julien Chaisse (2023).*	*Practice: Compare and contrast the primary sources of international law relevant to cyber conflicts, such as treaties, customary international law, general principles, and judicial decisions with the Tallinn Manual's recommendations.*	*Practice: Analyze the case of Shreya Singhal v. Union Of India AIR 2015 SC 1523, and highlight the observations of Altamas Kabir, CJ. with regards to the balance between freedom of expression and causing nuisance online.*

SLO-18	*Practice: Explore the recent policy changes that have aimed towards the incorporation of artificial intelligence in e-governance.*	*Practice: Explain the working of international depositary authorities under the Budapest Treaty on the International Recognition of the Deposit of Microorganisms.*	*Practice: Perform an ILAC analysis on possible real-world problem scenarios involving data leaks and privacy breaches.*	*Practice: Analyze recent cases or studies related to child sexual abuse committed through digital means, such as online grooming, sextortion, or distribution of child sexual abuse material.*	*Practice: Pick a recent incident where there has been a conflict between freedom of expression and content moderation under the Intermediary Guidelines and Ethics Code in India, relating to fake news and/or hate speech.*
Assessment	*Continuous Learning Assessment - 1*			*Continuous Learning Assessment - 2*	
	Continuous Learning Assessment - 3				

Resources			
1	Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd.	2	Information Warfare and Security by Dorothy F. Denning, Addison Wesley.
3	Carrie Morgan Whitcomb, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, 1 International Journal of Digital Evidence (2002).	4	Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd.
5	Data Privacy Principles and Practice by Natraj Venkataramanan and Ashwin Shriram, CRC Press.	6	Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers.
7	Information Security Governance, Guidance for Information Security Managers by W. KragBrothy, 1st Edition, Wiley Publication.	8	Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform. (Pearson , 13th November, 2001)
9	Auditing IT Infrastructures for Compliance by Martin Weiss, Michael G. Solomon, 2nd Edition, Jones Bartlett Learning.	10	Alexandra Perloff-Giles, Transnational Cyber Offenses: Overcoming Jurisdictional Challenges, The Yale Journal of International Law, 2018, available at https://bpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2018/02/191_Transnational-Cyber-Offenses-2i9mpg2.pdf.

Rationale (CLR)	*The purpose of learning this course is to:*	Depth				Attainment			Program Learning Outcomes (PLO)												
		1	2	3	4	1	2	3	1	2	3	4	5	6	7	8	9	10	11	12
CLR-1	*Introduce students to the various stakeholders involved in governing the internet at the international level. It covers technical standards, domain name management, and the role of different organizations such as IETF, ISOC, ICANN, ITU, IGF, OECD, and others. By exploring these topics, students will gain insight into how decisions are made regarding the infrastructure and architecture of the internet.*	Conceive	Design	Implement	Operate	Level of Thinking	Expected Proficiency (%)	Expected Attainment (%)	Disciplinary Knowledge	Critical Thinking	Problem Solving	Analytical Reasoning	Research-related Skills	Communication Skills	Cooperation/Team Work	Digital Literacy	Self-directed Learning	Moral and Ethical Reasoning	Leadership Qualities	Life Long Learning
CLR-2	*Delve into the specific legal frameworks that regulate e-commerce activities. Topics include conventions, model laws, working groups, and intellectual property protections related to online transactions. These concepts are crucial for understanding the rules that guide business practices across borders.*																				
CLR-3	*Examine international human rights instruments and EU regulations aimed at protecting individuals' personal information and their right to privacy. Studying these documents provides insights into best practices and emerging trends in data protection.*																				
CLR-4	*Explore the various international conventions, treaties, and protocols designed to combat cyber threats and protect vulnerable populations from harm. Examining these agreements highlights the importance of cross-border cooperation and collaboration in addressing transnational challenges.*																				
CLR-5	*Focus specifically on India's approach to regulating information technology and e-commerce through legislation like the IT Act 2000, its amendments, and other relevant guidelines. Comparing Indian law with international norms allows students to understand similarities and differences between jurisdictions while considering potential implications for businesses operating within those boundaries.*																				
Outcomes (CLO)	*At the end of this course, learners will be able to:*																				
CLO-1	*Analyze the role of international organizations such as IETF, ISOC, ICANN, ITU, WIPO, and others in governing the internet, e-commerce resources, privacy and data protection, and combating cybercrime, cyber warfare, and cyberterrorism.*	▯	▯		-	2	85	75	3	-	-	1	-	3	-	2	2	1	2	3
CLO-2	*Evaluate the significance of various legal instruments including treaties, conventions, model laws, protocols, regulations, and rules at the national and international level related to internet governance, e-commerce resources, privacy and data protection, and combating cybercrime, cyber warfare, and cyberterrorism.*	▯	▯	▯	-	2	85	75	3	3	1	2	2	3	2	1	2	1	2	3
CLO-3	*Develop evidence-based arguments regarding current issues and debates surrounding internet governance, e-commerce resources, privacy and data protection, and combating cybercrime, cyber warfare, and cyberterrorism using relevant theories, concepts, and frameworks from law, technology, policy, and ethics.*	▯	▯	▯	▯	3	85	75	3	1	3	1	3	3	2	1	1	2	1	3
CLO-4	*Communicate effectively both orally and in writing about complex topics related to internet governance, e-commerce resources, privacy and data protection, and combating cybercrime, cyber warfare, and cyberterrorism.*	▯	▯	▯	▯	3	85	75	3	3	2	3	3	3	-	2	3	3	3	3
CLO-5	*Apply critical thinking skills to assess the challenges and opportunities presented by globalization and digitization in relation to internet governance, e-commerce resources, privacy and data protection, and combating cybercrime, cyber warfare, and cyberterrorism.*	▯	▯	▯	▯	3	85	75	3	3	2	3	3	3	-	3	3	3	3	3

Assessment Method (Max. Marks: 100)													
		Continuous Learning Assessment (CLA 40% Weightage)								Final Exam	
Level of Thinking		Model Exam (20%)		Assignment/ Seminar/Group discussion/ Presentation		Participation in seminar/ Conference/ Publication		Participation in class room/co-curricular & Para curricular activities			
		(20%)		(10%)		(5%)		(5%)		(60%)	
1	Remember	40%	-	40%	-	30%	-		-	40%	-
2	Understand										
3	Apply	40%	-	40%	-	40%	-		-	40%	-
4	Analyze										
5	Evaluate	20%	-	20%	-	30%	-		-	20%	-
6	Create										
Total		100 %		100 %		100 %		100 %		100 %	

Strategies					
Technology		Pedagogy / Andragogy		Sustainable Development	
Simulations	☐	Clarification/Pauses	☐	Good Health & Well Being	☐
Presentation Tools					
Learning Management System		Group Discussion	☐	Quality Education	☐
		Hands-on Practice	☐		
		Debate	☐		
		Interactive Lecture	☐		
		Brainstorming	☐		

Designers					
Professional Experts		Higher Institution Experts		Internal Experts	
1	*<name>, <industry name>, <email id>*	1	*<name>, <institution name>, <email id>*	1	*<name>, SRMIST, <email id>*
2	*<name>, <industry name>, <email id>*	2	*<name>, <institution name>, <email id>*	2	*<name>, SRMIST, <email id>*

Code	PLCS24301T	Title	LEGAL RESEARCH METHODOLOGY	Category		Core Foundation	L	T	P	C
							3	1	2	5

Course Offering Department	School of Law	Prerequisite Courses		Co-requisite Courses		Progressive Courses		Data Book / Codes/Standards	

Title & Content	LEGAL EDUCATION	TEACHING AND EXAMINATION	RESEARCH	RESEARCH PROCESSES	ANALYSIS AND REPORT WRITING
Duration (hour)	18	18	18	18	18
SLO-1	*Comprehend the historical evolution of legal education from ancient times to the present day, including key milestones.*	*Comprehend various methods of teaching used in legal education, including their objectives, principles, and application in different contexts.*	*Comprehend the meaning and purpose of research in the field of law.*	*Comprehend the importance of conducting a comprehensive review of existing literature.*	*Comprehend the principles of statistical analysis and its application to legal research.*
SLO-2	*Examine the primary objectives of legal education, including preparing students for the legal profession, promoting critical thinking and analytical skills, fostering ethical values and professionalism, and advancing justice and the rule of law.*	*Examine the concept of problem method of teaching as an active learning approach, that involves presenting students with real-life legal problems to solve.*	*Examine and articulate the objectives of legal research.*	*Examine the formulation of research design such as experimental, correlation, descriptive, and qualitative designs that aligns with their research objectives, questions, and methodology.*	*Explore the interpretation of collected data .*
SLO-3	*Analyze the key provisions and standards outlined in the Part IV of the Bar Council of India Regulations 2008, pertaining to legal education and training requirements for aspiring lawyers.*	*Comprehend the concept of seminar method of teaching, which involves students conducting research, presenting findings, and engaging in scholarly discourse on specific legal topics.*	*Analyze the different types of research methodologies employed in legal and research, including qualitative, quantitative, mixed-methods, doctrinal, empirical, and comparative research.*	*Examine various methods of data collection used in legal research, including surveys, interviews, observations, document analysis, and archival research.*	*Explore and interpret the results of statistical analysis and evaluate their implications for legal theory, practice, and policymaking.*

SLO-4	*Tutorial: Conduct an in depth analysis and discussion on the evolution and objectives of legal education.*	*Tutorial: Conduct an in-depth analysis and discussion on the* strengths, limitations, and suitability of each teaching method for enhancing student learning and engagement.	*Tutorial: Conduct an in depth discussion on different types of research methodologies employed in legal research.*	*Tutorial: Conduct an in-depth discussion on review of literature and research design .*	*Tutorial: Conduct an in-depth discussion on statistical analysis.*
SLO-5	*Practice: Discuss the factors shaping the evolution of legal education, such as societal needs, technological advancements, globalization, and legal reforms.*	*Practice: Discuss how the problem method promotes critical thinking, problem-solving skills, and practical application of legal principles.*	*Practice: Discuss the role of research in generating new knowledge, addressing questions, and solving problems in the legal field and society at large.*	*Practice:* Engage in hands-on exercise by reviewing the existing literature and identifying the research gap.	*Practice: Discuss statistical analysis including data collection, organization, summarization, and interpretation.*
SLO-6	*Practice: Examine the effectiveness of legal education in developing practical legal skills and gaining real-world experience.*	*Practice: Discuss how the seminar method promotes independent research, oral presentation skills, and critical analysis of legal literature.*	*Practice: Discuss the characteristics, strengths, and limitations of each research type and their suitability for different research objectives and contexts.*	*Practice:* Engage in hands-on exercise by formulating *research designs for identified legal issues .*	*Practice: Discuss the various methods of interpretation of data collection .*
SLO-7	*Comprehend the role of the University Grants Commission (UGC) in regulating and overseeing higher education, including legal education, in India.*	*Comprehend the concept of discussion method which involves interactive exchanges among students and between students and instructors to explore legal concepts, cases, and issues.*	*Comprehend the social science research methods and their application to legal studies, including approaches such as surveys, interviews, case studies, content analysis, and ethnography.*	*Examine the quantitative methods of data collection*	*Comprehend the concept of hypothesis testing and its role in scientific inquiry and empirical research.*
SLO-8	*Examine the role of the state government, judiciary, legal profession, and other institutions in shaping legal education policies, standards, and practices.*	*Analyze the concept of socratic method which is characterized by a dialogue between instructor and students that challenges assumptions, promotes critical thinking, and encourages students to articulate and defend their viewpoints.*	*Examine distinct characteristics of legal research, including its focus on legal norms, principles, doctrines, and institutions.*	*Examine the qualitative methods of data collection.*	*Examine how to write research reports that effectively communicate the findings of their research projects.*

SLO-9	*Analyze the impact of UGC, state government and other institutions on legal education .*	*Comprehend the concept of Case law method of teaching, which involves studying legal cases in-depth to understand legal principles, doctrines, and precedents.*	*Gain an understanding of socio legal research which integrates legal analysis with insights from social sciences to examine the impact of law on society and vice versa.*	*Analyze sampling techniques used in legal research, including probability and non-probability sampling methods.*	*Explore the principles of clarity, coherence, and accuracy in report writing.*
SLO-10	*Tutorial: Conduct in-depth discussions on the role of UGC and other institutions in promoting legal education.*	*Tutorial: Conduct in-depth discussions on different methods of teaching .*	*Tutorial:Conduct in-depth discussions on socio legal research .*	*Tutorial – Conduct in-depth discussions on the strengths, limitations, and ethical considerations associated with each data collection method and select the most suitable approach based on their research objectives and constraints.*	*Tutorial – Conduct in-depth discussions on each hypothesis testing and select the most appropriate test based on their research design and objectives.*
SLO-11	*Practice: Discuss the contributions and responsibilities of these entities in promoting quality legal education, access to justice, and professional development*	*Practice: Discuss how the discussion method fosters collaboration, communication skills, and deeper understanding of legal principles through peer learning.*	*Practice: Discuss how social science research methods can be used to investigate legal phenomena, understand human behavior, and inform legal policymaking.*	*Practice:* Engage in hands-on exercise by collecting data for identified legal issues by employing qualitative data collection	*Practice: Engage in* hands-on exercise by testing the formulated hypotheses
SLO-12	*Practice: Discuss the gaps and challenges in promoting quality legal education including outdated curriculum ,ethical and professionalism deficits .*	*Practice: Discuss the effectiveness of the Socratic method in fostering intellectual curiosity, analytical skills, and confidence in legal reasoning.*	*Practice: Discuss how socio-legal research methods can be used to explore complex legal issues, understand legal processes, and evaluate the effectiveness of legal reforms.*	*Practice:*.Engage in hands-on exercise by collecting data for identified legal issues by employing qualitative data collection	*Practice: Engage in* hands-on exercise by writing research reports.
SLO-13	*Comprehend the recommendations on legal education made by the National Knowledge Commission (NKC), a high-level advisory body to the Government of India.*	*Comprehend various methods of examination and evaluation used in legal education, including written exams, essays, presentations, and practical assessments.*	*Comprehend the process of identifying research gaps, formulating research problems based on theoretical and practical considerations.*	*Comprehend the various sources of* legal material including statutes, subordinate legislation, notifications, policy statements. decisional material, foreign Judgments, legal databases.	*Comprehend and analyze the common statistical and experimental tests used in legal research, including the chi square test, T test ,Anova tests*

SLO-14	*Analyze the findings and recommendations of the 184th Report of the Law Commission of India (LCI) on legal education reforms.*	*Explore extension activities such as clinical programs, legal aid clinics, legal literacy initiatives, and participation in law reforms.*	*Comprehend the concept of hypothesis in research, including its role in formulating testable propositions and guiding empirical investigations.*	*Analyze the importance of the reports of various commissions and committees in legal research.*	*Examine the ethical principles and standards governing research conduct, including honesty, integrity, objectivity, and respect for human subjects.*
SLO-15	*Analyze and examine the recommendations of various committees and commissions tasked with reviewing and reforming legal education in India.*	*Comprehend various law reforms related to legal education .*	*Comprehend the formulation of clear, specific, research questions,that align with the objectives and scope of the research project.*	*Identify and analyze the challenges involved in the research process.*	*Identify the ethical considerations in legal research, such as informed consent, confidentiality, conflicts of interest, and data integrity.*
SLO-16	*Tutorial: Conduct an in depth discussion on the Law Commission of India's recommendations and their potential impact on legal education policy, curriculum development, and institutional governance.*	*Tutorial: Conduct an in depth discussion on the* various *assessment and evaluation methods suited for the legal field.*	*Tutorial:* Conduct an in-depth discussion on identifying research gaps, formulating hypothesis and framing research questions	*Tutorial:* Conduct an in depth discussion on primary legal sources to understand legal principles, doctrines, and precedents relevant to their research topic.	*Tutorial: Conduct in-depth discussions on the structure and components of research reports, including the introduction, literature review, methodology, results, discussion, and conclusion sections.*
SLO-17	*Practice: Discuss the implementation challenges of the recommendations of the Law Commission of India and their implications for legal education stakeholders.*	*Practice: Discuss the principles of fair assessment, feedback mechanisms, and strategies for promoting academic integrity and rigor.*	*Practice:* Engage in hands-on exercise by framing the hypothesis for any legal issues	*Practice: Discuss various stages of research including the review of literature, research design.*	*Practice: Discuss various ethical principles associated with legal research.*
SLO-18	*Practice: Discuss the implementation challenges of National Knowledge Commission recommendations.*	*Practice: Discuss the role of extension activities in bridging the gap between theory and practice, promoting access to justice, and fostering social responsibility among law students.*	*Practice:* Engage in hands-on exercise by framing *the research question for* any legal issues	*Practice: Discuss the various stages of research including data collection methods, sampling techniques, and sources of legal and decisional material.*	*Practice:* Engage in hands-on exercise by conducting the research related to the identified legal area .

Resources			
1	*WilliamJ. Goode and Paul K. Hatt, Methods in Social Research (2017)*	2	*Adam Podgorecki, Law and Society, Routledge & Kagal Paul, London, 1974*
3	*Prof.P. IshwaraBhat, Idea and Methods of Legal Research (2019)*	4	*Anwarul Yaqin, Legal Research and Writing Methods (2008)*
5	*S.K.Verma, M. Afzal Wani, Legal Research and Methodology, Indian Law Institute (2010)*		

Rationale (CLR)	*The purpose of learning this course is to:*	Depth				Attainment			Program Learning Outcomes (PLO)												
		1	2	3	4	1	2	3	1	2	3	4	5	6	7	8	9	10	11	12
		Conceive	Design	Implement	Operate	Level of Thinking	Expected Proficiency (%)	Expected Attainment (%)	Disciplinary Knowledge	Critical Thinking	Problem Solving	Analytical Reasoning	Research-related Skills	Communication Skills	Cooperation/Team Work	Digital Literacy	Self-directed Learning	Moral and Ethical Reasoning	Leadership Qualities	Life Long Learning
CLR-1	*To acquire a foundational understanding of the evolution of legal education, including the objectives outlined by the Bar Council of India (BCI) Regulations of 2008, as well as the roles of various institutions such as the University Grants Commission (UGC), the State, and other relevant bodies, also, the 184th report of National Knowledge Commission (NKC) on Legal Education, offer insights into the challenges faced by the legal education system and proposed reforms to address them.*																				
CLR-2	*Equip participants with various methods of teaching, including the Problem Method, Discussion Method, Seminar Method, Socratic Method, and Case Method, as well as techniques for examination and evaluation. Additionally, participants will explore extension activities such as clinical work, legal aid, legal literacy, and involvement in law reforms.*																				
CLR-3	*Provide participants with a comprehensive understanding of the concept of research, its objectives, and various types, including social science research, legal research, and socio-legal research. Additionally, participants will be equipped with knowledge and skills for identifying research problems, framing hypotheses, and formulating research questions.*																				
CLR-4	*Equip participants with comprehensive knowledge and practical proficiency in several key areas essential for conducting high-quality research including* Review of Literature, Formulation of Research Design,hypothesis,methodology, data collection .																				
CLR-5	*Equip participants with advanced proficiency in statistical and legal analysis of data, interpretation and implication of data, hypothesis testing, report writing, statistical and experimental tests in research, research ethics, and integrity, to empower them for dynamic legal research.*																				

Outcomes (CLO)	At the end of this course, learners will be able to:																						
CLO-1	*Gain a foundational understanding of the evolution, objectives, regulations, and stakeholders involved in legal education in India. Develop a comprehensive understanding of legal education policies, standards, and reforms in India, enabling them to contribute effectively to the advancement of legal education and the legal profession.*				-	2	85	75	3	-	-	1	-	3	-	2	2	1	2	3
CLO-2	*Gain comprehensive understanding of effective teaching methods, assessment practices, and extension activities in legal education, also enhance learning, engagement, and professional development in the field of law.*				-	2	85	75	3	2	1	2	2	3	-	1	2	1	2	3
CLO-3	*Enhance their research skills and capabilities, enabling them to conduct rigorous and impactful research in their respective fields of study or professional practice.*					3	85	75	3	1	3	1	3	3	-	1	1	2	1	3
CLO-4	*Critically evaluate existing literature, design and execute research projects, and contribute to the advancement of knowledge in the legal field. Navigate the complexities of research design, data collection, and analysis, as well as effectively utilize legal materials and other relevant sources to produce high-quality research outputs.*					3	85	75	3	3	2	3	3	3	-	2	3	3	3	3
CLO-5	*Develop advanced research skills and competencies necessary for conducting rigorous and ethically sound legal research. Equipped to analyze legal data, test research hypotheses, communicate research findings, and contribute to evidence-based decision-making in the legal profession and academia.*					3	85	75	3	3	2	3	3	3	-	3	3	3	3	3

Assessment Method (Max. Marks: 100)											
Level of Thinking		Continuous Learning Assessment (CLA 40% Weightage)								Final Exam	
		Model Exam (20%)		Assignment/ Seminar/Group discussion/ Presentation		Participation in seminar/ Conference/ Publication		Participation in class room/co-curricular & Para curricular activities			
		(20%)		(10%)		(5%)		(5%)		(60%)	
1	Remember	40%	-	40%	-	30%	-		-	40%	-
2	Understand										
3	Apply	40%	-	40%	-	40%	-		-	40%	-
4	Analyze										
5	Evaluate	20%	-	20%	-	30%	-		-	20%	-
6	Create										
Total		100 %		100 %		100 %		100 %		100 %	

Strategies					
Technology		Pedagogy / Andragogy		Sustainable Development	
Simulations	✓	Clarification/Pauses	✓	Quality Education	✓
Presentation Tools	✓	Case studies	✓	Decent Work and Economic Growth	✓
Learning Management System	✓	Group Discussion	✓	Reduced Inequalities	✓
		Group task	✓		
		Debate	✓		
		Interactive Lecture	✓		

Designers					
Professional Experts		Higher Institution Experts		Internal Experts	
1		1	*DR. REDDIVARI REVATHI* (Former HOD , Department of constitutional law , in School of Excellence in Law)	1	*Prof.(Dr.)Sree Sudha, Dean, School of Law, SRMIST*
2		2	*DR. MANJULA* (Assistant Professor, School of Excellence in Law)	2	

Code	PLCS24302T	Title	CYBER FORENSICS & EVIDENCIAL ISSUES	Category		Professional Core	L	T	P	C
							3	1	2	5

Course Offering Department	School of Law	Pre-requisite Courses		Co-requisite Courses		Progressive Courses		Data Book / Codes/Standards	

Title & Content	Unit 1	Unit 2	Unit 3	Unit 4	Unit 5
Duration (hour)	18	18	18	18	18
SLO-1	*Explain the fundamental concepts and importance of forensic science in criminal investigations and legal proceedings.*	*Analyze and classify different computing systems using system-based categorization techniques.*	*Define and classify different types of digital data (non-volatile and volatile) used in forensic analysis, and explain their significance in an investigation.*	*Explain the importance of reliability in the evidential aspect of cyber forensics and how it applies to the collection, preservation, and analysis of digital evidence.*	*Explain the concept of relevance in the context of electronic evidence and understand its importance in cyber forensic investigations.*
SLO-2	*Identify various types of physical evidence, including their classification, characteristics, and significance in crime scene analysis and interpretation.*	*Identify common Windows Systems products and their associated artifacts for digital forensic investigations.*	*Identify various methods and techniques to recover deleted or corrupted electronic data, including analyzing slack space, unallocated clusters, and using file carving tools.*	*Identify best practices for recovering and preserving digital evidence to ensure its integrity and admissibility in court.*	*Apply sections 5, 45A, 46, 47A, and 51 of the Indian Evidence Act to determine the relevance of electronic evidence in legal proceedings.*
SLO-3	*Describe Locard's Exchange Principle and its role in collecting and analyzing physical evidence.*	*Explain the purpose and use of various Linux system artifacts in a digital forensic examination.*	*Apply best practices for extracting data from a variety of sources such as hard drives, mobile devices, and cloud storage services while maintaining the integrity of the original source.*	*Analyze digital evidence using appropriate tools and techniques while maintaining a thorough documentation trail.*	*Understand the principles governing admissibility of electronic evidence under various sections of the Indian Evidence Act including sections 3, 65A, 65B, 67A, 73A, 85A, 85B, 85C, 88A, and 90A.*
SLO-4	*Tutorial: Seminar on the Strengths and Criticisms against Locard's Exchange Principle.*	*Tutorial: Seminar on commonly used computer architectures such as x86, ARM, MIPS, PowerPC, and SPARC.*	*Tutorial: Seminar on the best practices involved in the extraction of lost data from hard drives, mobile devices, and cloud storage services while maintaining the integrity of the original source.*	*Tutorial: Seminar on common cybersecurity lapses and how to tackle them.*	*Tutorial: Seminar on the changes brought about by the Bharatiya Sakshya Adhiniyam, 2023 with respect to admissibility of electronic evidence.*

SLO-5	*Practice: Visit any Court having jurisdiction near SRM's locality when there is a posting for any criminal trial involving the examination of a forensic expert. Write a Brief Report on your observations.*	*Practice: Learn to identify an OS by examining file system structures, installed software packages, or running processes; identifying these OSs without relying solely on obvious clues such as file names containing "Windows" or "Linux."*	*Practice: Write a brief summary on the different methods and techniques for recovering deleted or corrupted electronic data, including analyzing slack space, unallocated clusters, and using file carving tools.*	*Practice: Choose a scenario where digital evidence needs to be recovered (e.g., a hacked email account, a compromised server, or a deleted file), and students must outline the steps they would take to recover and preserve the evidence according to best practices.*	*Practice: Perform an ILAC Analysis on the case of Anvar P.V. v. P.K. Basheer & Ors (2014) 10 SCC 473, and emphasize on the importance of veracity and reliability of electronic evidence.*
SLO-6	*Practice: Analyze how the Locard's Exchange Principle was applied in the sensational 'Weimar Children Murder' case.*	*Practice: Recover the internet history data from a provided Windows or Linux system, using built-in tools like Microsoft's Internet Explorer History, Google Chrome history database, Mozilla Firefox places.sqlite, or third-party solutions if necessary, and examining timestamps, visited URLs, downloaded files, cookies, cache, browsing habits, and other potentially useful information related to user activity.*	*Practice: Conduct a hands-on examination of a sample computer system, and Identify the different types of digital data based on their characteristics as either non-volatile or volatile data.*	*Practice: Compare the legal requirements for presenting digital evidence in courts in India and any other jurisdiction.*	*Practice: Critically analyze provisions under Indian evidence law governing presumption of electronic messages, electronic records, digital signatures, proof as to contents of electronic documents.*
SLO-7	*Understand the differences between tangible and intangible forms of evidence, with a focus on the unique challenges associated with identifying, preserving, and examining cyber evidence.*	*Compare and contrast the features and components of Mac OS X systems and artifacts relevant to digital forensics.*	*Utilize forensic imaging and duplication tools to create exact copies of digital media for further analysis without altering the original data.*	*Evaluate the validity of forensic tools used in the examination of digital evidence, taking into account any relevant standards or guidelines established by organizations such as NIST and SWGDE.*	*Analyze legal standards determining admissibility of electronic evidence in courts, specifically focusing on the Daubert Test and the Kumho Decision.*
SLO-8	*Analyze the application of cyber forensics in detecting, preventing, and prosecuting digital crimes, such as hacking, phishing, and identity theft.*	*Evaluate the importance of analyzing web browser data as part of a comprehensive digital investigation.*	*Investigate internet and networking activities by analyzing logs, metadata, and other artifacts left behind by users and applications.*	*Understand the role of NIST and SWGDE in establishing standards and guidelines for digital forensics, including the validation of forensic tools.*	*Evaluate the role of authentication as a condition for admissibility of electronic evidence in Indian courts and identify methods to ensure authenticity.*

SLO-9	*Investigate the basics of computer hardware, software, and networks, including an overview of common components like processors, motherboards, hard disks, and operating systems.*	*Investigate computer networks and analyze network traffic using principles of computer network forensics.*	*Trace IP addresses and email headers to identify the originator, recipient, and path taken during communication.*	*Compare and contrast the two main approaches to forensic tool validation: Tool Oriented Approach and Functional Oriented Approach.*	*Distinguish between primary and secondary evidence and apply relevant provisions of the Indian Evidence Act related to admissibility of secondary evidence in case of unavailability or difficulty in producing primary evidence.*
SLO-10	*Tutorial: Group Discussion on Evidentiary Issues in Cyberspace Transactions.*	*Tutorial: Seminar on Essential Digital Forensic Artifacts such as registry keys, system logs, email archives, memory dumps, and internet history.*	*Tutorial: Expert seminar on the use of forensic imaging and duplication tools.*	*Tutorial: Expert Talk on the Roles of NIST (National Institute of Standards and Technology) and SWGDE (Scientific Working Group on Digital Evidence) in establishing standards and guidelines for digital forensics.*	*Tutorial: Seminar on practical applications primary and secondary evidence in cyberspace.*
SLO-11	*Practice: Students must create two lists, one for tangible cyber evidence and another for intangible cyber evidence. Label them List A (Tangible) and List B (Intangible). For each list, provide at least five examples of items that could be considered evidence in a cybercrime investigation.*	*Practice: Choose two popular web browsers (e.g., Google Chrome and Mozilla Firefox), install both on a system, and browse various websites, perform searches, and utilize bookmarks; and test different scenarios including private/incognito mode usage; performing an analysis of stored data created by each browser, focusing on aspects such as cookies and history records.*	*Practice: Create an exact copy of a USB drive using forensic imaging and duplication tools, using Write blocker hardware (e.g., Tableau T8u), a Forensic image creation software (e.g., FTK Imager or Guymager).*	*Practice: Write a one-page summary outlining the roles of NIST and SWGDE in digital forensics, focusing on their contributions to setting standards and guidelines for forensic tool validation.*	*Practice: Critically analyze the way the Daubert Standard laid down in the case of Daubert v. Merrell Dow Pharmaceuticals Inc. 509 U.S. 579 (1993), supplanted the Frye Standard laid down in the case of Frye v. United States, 293 F. 1013 (D.C. Cir. 1923).*

SLO-12	*Practice: Problem scenario analysis where an employee is accused of stealing sensitive data from their employer. Analyze what types of tangible and intangible evidence could be used in this case. Discuss the potential challenges faced while collecting, analyzing, and presenting these pieces of evidence in court such as chain-of-custody, privacy concerns, legal restrictions, etc.*	*Practice: Brief Write-Up comparing and contrasting Features and Components of Mac OS X Systems and Artifacts Relevant to Digital Forensics.*	*Practice: Write a brief write-up on the importance of tracing IP addresses and email headers to identify the originator, pathway of communication, and the recipient.*	*Practice: Students may be provided access to two different forensic tools, Tool A and Tool B, both having the capability to perform similar functions but developed by different developers. Students must compare and contrast these tools' capabilities and validate them according to NIST and SWGDE guidelines.*	*Practice: Brief Write-Up of the role of CCTV footage as secondary evidence.*
SLO-13	*Compare and contrast different types of networking systems, such as Personal Area Networks (PAN), Local Area Networks (LAN), Metropolitan Area Networks (MAN), and Wide Area Networks (WAN).*	*Differentiate between different types of networks (e.g., LAN, WAN), network classes (A, B, C), and subnet masks used for addressing and routing in modern internetworks.*	*Conduct comprehensive web investigation and analysis, including search engine queries, social media activity, and website visit history.*	*Apply the concept of chain of custody to digital evidence and explain its significance in ensuring the reliability and admissibility of said evidence.*	*Assess the challenges faced by judges and lawyers while dealing with electronic evidence in court proceedings and propose solutions to overcome these issues.*
SLO-14	*Evaluate the impact of cloud computing on forensic investigations, including best practices for data acquisition, analysis, and presentation in court.*	*Apply knowledge of network hardware devices such as routers, switches, and firewalls to conduct network forensic examinations.*	*Analyze instant messaging conversations, file transfers, and other forms of online communication to gather intelligence and build cases against suspects.*	*Critique the strengths and weaknesses of various methods for maintaining chain of custody in digital forensics investigations.*	*Compare and contrast the approaches towards admitting electronic evidence in different jurisdictions such as the US and India and evaluate their implications.*

SLO-15	*Apply theoretical knowledge to practical scenarios by conducting simulated forensic analyses using industry-standard tools and techniques.*	*Examine and mitigate network threats and vulnerabilities through an understanding of IP security architectures and web security concepts.*	*Examine file sharing networks, peer-to-peer protocols, and cloud computing environments to locate and collect evidence related to illegal activities such as copyright infringement, intellectual property theft, and child pornography. Additionally, students will learn how to preserve digital evidence securely throughout the investigation process to ensure its admissibility in court.*	*Synthesize the concepts of reliability, evidence recovery, preservation, analysis, validity of forensic tools, and chain of custody to develop a comprehensive approach to digital forensics that prioritizes accuracy and credibility.*	*Develop best practices for handling electronic evidence during investigation, preservation, and presentation stages to ensure compliance with legal requirements and improve the chances of acceptance in court.*
SLO-16	*Tutorial: Simulation using industry-standard tools like Autopsy, EnCase, or FTK, demonstrating to the students a simulated forensic analysis involving cloud-stored data.*	*Tutorial: Group Discussion on threat mitigation strategies such as intrusion detection systems (IDS) and intrusion prevention systems (IPS) etc.*	*Tutorial: Seminar on the state of safe Cloud Computing in the 21st Century.*	*Tutorial: Expert Talk on the concepts of reliability, evidence recovery, preservation, analysis, validity of forensic tools, and chain of custody.*	*Tutorial: Seminar on the need for training to judges and lawyers on the technical aspects of electronic evidence so they can better assess its reliability.*
SLO-17	*Practice: Research each network type studied in this unit - PAN, LAN, MAN, and WAN - and create a table or chart that outlines their key characteristics such as size, speed, security, cost, topology, protocols used, etc.*	*Practice: Classify a set of given IP addresses into categories A, B, and C, by converting them into binary format.*	*Practice: Perform a thorough web investigation and analyze the results to gain insights into any famous internet celebrity to assess their online presence and behavior.*	*Practice: Create a chain of custody log for a hypothetical digital device (e.g., a smartphone or a laptop) involved in a criminal investigation. Document each step of the process from seizure to storage to analysis, including the date, time, personnel involved, actions taken, and any changes made to the device or its contents.*	*Practice: Write a report on how digital signatures, timestamps, and other metadata can be used to establish authenticity of electronic records.*
SLO-18	*Practice: Brief report discussing potential challenges in preserving admissibility of cloud-based evidence in legal proceedings.*	*Practice: Investigate a reported case of potential unauthorized SSH access to a server within an organization's internal network; looking for signs of anomalous behavior such as multiple failed login attempts, unusual geographical origin of connection requests, unexpected timing patterns, etc.*	*Practice: Write a Brief on the essentials to be followed for preserving and maintaining the admissibility of electronic evidence in cybercrimes.*	*Practice: Critiquing the various methods for maintaining chain of custody in digital forensics investigations, such as Physical Seizure & Storage, Hashing Algorithms, Imaging Techniques, Access Controls & Auditing, and Encryption & Secure Transmission.*	*Practice: Brief write-up on how electronically stored information digital forensic investigation*

Assessment	*Continuous Learning Assessment - 1*	*Continuous Learning Assessment - 2*
	Continuous Learning Assessment - 3	

Resources			
1	Carrie Morgan Whitcomb, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, 1 International Journal of Digital Evidence (2002).	2	Brian Carrier, Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers, 1 International Journal of Digital Evidence, 1 (2003).
3	Larry Daniel and Lars Daniel, Digital Forensics for Legal Professionals (Elsevier 2012).	4	Cory Altheide and Harlan Carvey, Digital Forensics with Open Source Tools (Elsevier 2011).
5	Josiah Dykstra, Forensic Collection of Electronic Evidence from Infrastructure: As A Service Cloud Computing, 19 Rich J L & Tech 1.	6	Laura Millar, Preserving Electronic Records (International Records Management Trust, 2009).
7	Brian Carrier, Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers, 1 International Journal of Digital Evidence, 3 (2003).	8	Yinghua Guo et al, Validation and Verification of Computer Forensic Software Tools–Searching Function, 6 Digital Investigation, p. 513 (2009).
9	André Årnes, Digital Forensics, Wiley, 2017.	10	Dr. Nilakshi Jain, Dr. Dhananjay R. Kalbande, Digital Forensic, Wiley, 2017.

Rationale (CLR)	*The purpose of learning this course is to:*
CLR-1	*Understand the fundamental concepts and principles of forensic science, including Locard's Exchange Principle, and their application in criminal investigation and adjudication. Students should also become familiar with the differences between tangible and intangible forms of evidence, particularly in the context of cyber forensics.*
CLR-2	*Gain knowledge about various system-based categories, such as Windows, Linux, and Mac OS X, and their respective artifacts. This includes an understanding of web browsers, computer network forensics, and the monitoring of computer network activities. Additionally, students will learn about emerging trends in forensic analysis, such as cloud forensics and mobile device analysis.*
CLR-3	*Learn about the tools and techniques used in digital forensics, including the recovery and examination of both non-volatile and volatile data. Students will gain hands-on experience in using forensic imaging, data extraction, and file carving tools to analyze various types of digital evidence.*
CLR-4	*Develop an understanding of the evidential aspects of cyber forensics, including the reliability and admissibility of digital evidence in court proceedings. Students will learn about legal standards determining admissibility, such as the Daubert Test and the Kumho Decision, as well as the role of national and international organizations like NIST and SWGDE in validating forensic tools.*
CLR-5	*Apply theoretical knowledge to practical scenarios by conducting simulated forensic analyses, interpreting results, and drawing conclusions based on findings, so that students will be able to develop critical thinking skills necessary to evaluate complex digital evidence and communicate findings effectively to diverse audiences.*

Outcomes (CLO)	*At the end of this course, learners will be able to:*	Depth				Attainment			Program Learning Outcomes (PLO)												
		Conceive	Design	Implement	Operate	Level of Thinking	Expected Proficiency (%)	Expected Attainment (%)	Disciplinary Knowledge	Critical Thinking	Problem Solving	Analytical Reasoning	Research-related Skills	Communication Skills	Cooperation/Team Work	Digital Literacy	Self-directed Learning	Moral and Ethical Reasoning	Leadership Qualities	Life Long Learning
		1	2	3	4	1	2	3	1	2	3	4	5	6	7	8	9	10	11	12
CLO-1	*Understand the fundamental concepts and principles of forensic science, including Locard's Exchange Principle, and their applications in both physical and cybercrime investigations.*	▯	▯		-	2	85	75	3	-	-	1	-	3	-	2	2	1	2	3
CLO-2	*Identify and classify various forms of evidence, including tangible and intangible evidence, and understand the importance of proper collection, recovery, and preservation techniques for each type.*	▯	▯	▯	-	2	85	75	3	2	1	2	2	3	-	1	2	1	2	3
CLO-3	*Analyze and interpret digital evidence found on computers, mobile devices, and networks using appropriate tools and methodologies, while adhering to ethical and legal guidelines.*	▯	▯	▯	▯	3	85	75	3	1	3	1	3	3	-	1	1	2	1	3
CLO-4	*Evaluate the reliability and admissibility of digital evidence according to national and international legal standards, with an emphasis on the role of NIST and SWGDE in validating forensic tools.*	▯	▯	▯	▯	3	85	75	3	3	2	3	3	3	-	2	3	3	3	3
CLO-5	*Apply critical thinking skills to evaluate the strengths and limitations of different approaches to cyberforensic analysis, drawing upon knowledge of relevant laws, regulations, and best practices.*	▯	▯	▯	▯	3	85	75	3	3	2	3	3	3	-	3	3	3	3	3

Assessment Method (Max. Marks: 100)																			
		Continuous Learning Assessment (CLA 40% Weightage)												Final Exam					
Level of Thinking		Model Exam (20%)				Assignment/ Seminar/Group discussion/ Presentation				Participation in seminar/ Conference/ Publication				Participation in class room/co-curricular & Para curricular activities					
		(20%)				(10%)				(5%)				(5%)				(60%)	
1	Remember	40%		-		40%		-		30%		-				-		40%	-
2	Understand																		
3	Apply	40%		-		40%		-		40%		-				-		40%	-
4	Analyze																		
5	Evaluate	20%		-		20%		-		30%		-				-		20%	-
6	Create																		
Total		100 %				100 %				100 %				100 %				100 %	

Strategies					
Technology		Pedagogy / Andragogy		Sustainable Development	
Simulations	▯	Clarification/Pauses	▯	Good Health & Well Being	▯
Presentation Tools	▯				
Learning Management System		Group Discussion	▯	Quality Education	▯
		Hands-on Practice	▯		
		Debate	▯		
		Interactive Lecture	▯		
		Brainstorming	▯		

Designers					
Professional Experts		Higher Institution Experts		Internal Experts	
1	*<name>, <industry name>, <email id>*	1	*<name>, <institution name>, <email id>*	1	*Dr. Ishita charterjee, Professor, School of law, SRMIST*
2	*<name>, <industry name>, <email id>*	2	*<name>, <institution name>, <email id>*	2	*<name>, SRMIST, <email id>*

Code	PLCS24303T	Title	PROCEDURAL ISSUES OF CYBER LAW	Category		Professional Core	L	T	P	C
							3	1	2	5

Course Offering Department	School of Law	Pre-requisite Courses		Co-requisite Courses		Progressive Courses		Data Book / Codes/Standards	

Title & Content	Jurisdictional issues	Issues connected with legal assistance and special investigative techniques	Issues based on extradition	Issues relating to the prosecution of transnational cybercrimes	Issues related to cyber forensics
Duration (hour)	18	18	18	18	18
SLO-1	*Define jurisdictional principles and distinguish them from traditional jurisdiction.*	*. Understand the concept of mutual legal assistance in the context of transnational crimes*	*Understanding UNTOC (United Nations Convention against Transnational Organized Crime) and its role in extradition of transnational offenders*	*Understand the challenges faced by prosecuting states in dealing with transnational cybercrimes.*	*Understand the key provisions of data protection laws such as GDPR and CCPA.*
SLO-2	*Analyze legislative, executive, and judicial jurisdiction in the context of transnational crimes.*	*Analyze the bilateral and multilateral treaties relevant to mutual legal assistance*	*Analysis of limitations of extradition - Exploring the checklist of extradition requirements*	*Recognize the complexities in evidence gathering across borders in transnational cybercrime cases.*	*Evaluate challenges faced by cyber forensic investigators in adhering to data privacy regulations.*
SLO-3	*Apply international law principles such as territoriality, nationality, and protective principle to transnational crimes.*	*Evaluate the role of UNTOC (United Nations Convention against Transnational Organized Crime) in facilitating mutual legal assistance*	*Overview of extradition principles and practices*	*Analyze the issues arising when a cybercrime affects multiple nations.*	*Analyze the importance of legal compliance in maintaining the admissibility of digital evidence in court.*
SLO-4	*Tutorial Discuss case studies illustrating different jurisdictional principles in practice.*	*Tutorial international cooperation mechanisms for confiscation purposes*	*Tutorial - Case studies and examples illustrating the application of dual criminality principle.*	*Tutorial :Case studies and discussions on the importance of international cooperation in cybercrime prosecution.*	*Tutorial :Discuss strategies for handling and storing digital evidence while respecting individuals' privacy rights.*
SLO-5	*Practice:Conduct simulated exercises to explore the application of territoriality principle in resolving jurisdictional conflicts.*	*Practice:Discuss the principles and practices of law enforcement cooperation in transnational crime investigations*	*Practice:Practical exercises on identifying cases where dual criminality principle applies - Mock scenarios to analyze the relevance of dual criminality in extradition cases*	*Practice:Research and presentation on the initiatives of CSCAP and similar organizations in combating cybercrimes.*	*Practice:Demonstrate proper collection techniques of digital evidence in compliance with data protection laws.*
SLO-6	*Practice:Analyze real-life scenarios involving subjective and objective territoriality*	*Practice:Examine the different types of special investigative techniques, including reactive,*	*Practice:Hands-on exercises on understanding and applying the rule of speciality in extradition*	*PracticeInvestigate the contributions of the Digital Opportunity Taskforce of G8 in*	*Practice:Simulate scenarios to practice ensuring the integrity of digital evidence in alignment with*

		proactive, and disruptive approaches	*cases - Role-playing scenarios to demonstrate the importance of rule of speciality*	*addressing cybercrime issues.*	*legal requirements.*
SLO-7	*Examine the concepts of active and passive nationality in determining jurisdiction.*	*Demonstrate skills in crime scene investigation techniques*	*Analysis of the autdedereaut judicare principle in extradition law - Understanding its significance in international criminal law*	*Identify additional challenges faced in prosecuting transnational cybercrimes, such as lack of specialized prosecutors.*	*Examine the implications of end-to-end encryption on cyber forensic investigations.*
SLO-8	*Explore the theory of rejecting territoriality and its implications for jurisdiction.*	*Understand the significance and challenges of joint investigations in transnational crime cases*	*Examination of the extradition of political offenders - Reviewing historical cases and their implications on current extradition practices*	*Assess the impact of the lack of cross-border evidence on cybercrime investigations and prosecutions.*	*Explore innovative decryption techniques and tools to overcome encryption challenges.*
SLO-9	*Evaluate general and specific personal jurisdiction, ubiquity jurisdiction, effect test, and sliding scale test.*	*Explore border control measures and their role in preventing transnational crimes*	*Demonstrate Role of bilateral and multilateral treaties in extradition - Case studies on treaty-based extradition mechanisms*	*Explore the importance of awareness among first responders in handling cybercrime incidents.*	*Discuss strategies for preserving data integrity in secure environments such as encrypted storage systems and blockchain networks.*
SLO-10	*TutorialEngage in group discussions to analyze jurisdictional challenges posed by emerging technologies.*	*TutorialEvaluate the legal and ethical implications of electronic surveillance*	*TutorialGuided walkthrough of the extradition checklist and procedure - Simulated exercises to understand the step-by-step process of extradition*	*Tutorial –: Discussion on the shortage of cyber forensic experts and its effects on cybercrime investigations.*	*Tutorial - Review case studies highlighting successful decryption methods used in cyber forensic investigations.*
SLO-11	*Practice:Simulate court proceedings to understand the jurisdictional implications of the Indian Penal Code and Information Technology Act.*	*Practice:the methodologies and challenges associated with undercover operations*	*PracticePractical scenarios to apply extradition laws and procedures - Group discussions on legal strategies in extradition cases*	*Practice:Simulation exercises on the challenges faced by investigators in cybercrime cases*	*Practice: Utilize decryption tools to access encrypted data in simulated forensic scenarios.*
SLO-12	*Practice:Explore jurisdictional issues through case studies based on the United Nations Convention against Transnational Organized Crimes.*	*Practice:Develop proficiency in expedited preservation of data techniques*	*Practice: - Analysis of human rights considerations in extradition cases - Debates and discussions on balancing extradition with human rights concerns*	*Practice:Assessment of educational initiatives aimed at enhancing capabilities in cybercrime investigation and prosecution.*	*Practice:Investigate methods for maintaining evidentiary value while analyzing digital evidence from secure environments.*
SLO-13	*Assess the jurisdictional competence of courts under the Indian Penal Code and Information Technology Act.*	*Understand the principles and procedures of real-time collection of communication traffic data*	*Overview of the Revised Manual on the Model Treaty on Extradition issued by UNODC - Understanding its implications on extradition practices*	*Analyze the complexity and cost factors involved in prosecuting transnational cybercrimes.*	*Identify challenges associated with IoT devices in forensic analysis.*
SLO-14	*Investigate jurisdictional challenges posed by international*	*Discuss the legal frameworks and safeguards concerning interception*	*Examination of the Model Law on Extradition by the United Nations*	*Assess the significance of private sector participation in combating*	*Discuss the complexities of investigating cybercrimes involving*

	treaties such as the United Nations Convention against Transnational Organized Crimes.	*of content data*	*Office on Drugs and Crime - Comparative analysis with existing extradition laws*	*cybercrimes.*	*cloud computing.*
SLO-15	*Discuss the role of jurisdiction in combating transnational organized crimes at the international level.*	*Assess the effectiveness and limitations of mutual legal assistance in the context of international cooperation (Lecture 9).*	*Discussion on emerging trends and challenges in extradition law - Reviewing recent case studies and their impact on extradition practices*	*Understand the importance of collaboration between public and private sectors in addressing cybercrime challenges.*	*Explore collaborative approaches between forensic experts and cloud service providers in cybercrime investigations.*
SLO-16	*Tutorial: Analyze legal precedents and case studies related to jurisdictional disputes in transnational crime cases.*	*Tutorial:Apply theoretical knowledge to practical scenarios through tutorial sessions (Tutorial 3).*	*Tutorial:Application exercises based on the Model Treaty and Model Law on Extradition - Group discussions on adapting model laws to specific legal contexts*	*Tutorial:Case studies and practical exercises on applying international legal frameworks in cybercrime prosecution.*	*Tutorial- Develop strategies for retrieving and analyzing data from interconnected IoT devices*
SLO-17	*Practice:Conduct mock trials to apply jurisdictional principles in resolving complex transnational crime cases.*	*Practice:Demonstrate competence in conducting practical exercises related to transnational crime investigation techniques (Practical 5).*	*Practice:Case analysis sessions focusing on legal strategies in extradition cases - Role-playing exercises to simulate legal proceedings in extradition hearings*	*Practice:: Role-playing exercises on overcoming jurisdictional hurdles in cybercrime investigations and prosecutions.*	*Practice:Simulate investigations into cybercrimes involving cloud services to understand jurisdictional challenges and access rights*
SLO-18	*Practice:Present research projects exploring jurisdictional issues in contemporary transnational crime scenarios.*	*Practice:Reflect on the ethical considerations and human rights implications of utilizing special investigative techniques (Practical 6).*	*Practice:ASimulated extradition proceedings based on real-life scenarios - Evaluation and feedback on participants' understanding of extradition law and procedures.*	*Practice:Development of recommendations for improving international cooperation and legal assistance mechanisms in cybercrime cases.*	*Practice:Collaborate with cloud service providers in a simulated forensic scenario to address chain of custody issues and ensure the integrity of digital evidence.*

Assessment	*Continuous Learning Assessment - 1*	*Continuous Learning Assessment - 2*
	Continuous Learning Assessment - 3	

Resources			
11	Kevin O'Shea et al., Cyber Crime Investigations: Bridging the Gaps Between, Security Professionals, Law Enforcement, and Prosecutors, Syngress Publishing, Inc. 2007 available at https://wcu.edu.az/uploads/files/Cyber%20Crime%20Investigations%20(%20PDFDrive%20).pdf	12	Darrel C. Menthe, Jurisdiction in Cyberspace: A Theory of International Spaces, 1998 available at https://core.ac.uk/download/pdf/232684908.pdf
13	Alexandra Perloff-Giles, Transnational Cyber Offenses: Overcoming Jurisdictional Challenges, The Yale Journal of International Law, 2018, available at https://bpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2018/02/191_Transnational-Cyber-Offenses-2i9mpg2.pdf	14	Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd.
15	Marinella Marmo, Nerida Chazal, Transnational Crime and Criminal Justice, Sage, 2016.	16	S Atya D. Bedi , Extradition In International Law And Practice (1966) Cambridge.
17	Neil Boister, An Introduction to Transnational Criminal Law, OUP	18	
19		20	.

Rationale (CLR)	*The purpose of learning this course is to:*	Depth				Attainment			Program Learning Outcomes (PLO)												
		1	2	3	4	1	2	3	1	2	3	4	5	6	7	8	9	10	11	12
CLR-1	*The course on jurisdictional principles and their application in transnational crimes offers learners a comprehensive understanding of legal authority beyond territorial boundaries. Through an exploration of legislative, executive, and judicial jurisdiction, participants gain insight into the multifaceted nature of legal frameworks in addressing cross-border criminal activities. By applying international law principles such as territoriality, nationality, and the protective principle, learners analyze and resolve jurisdictional conflicts effectively, equipping them with the skills to navigate complex legal scenarios involving multiple jurisdictions.*																				
CLR-2	*Understanding mutual legal assistance in transnational crimes enables investigators to navigate legal frameworks, treaties, and UN conventions effectively. It fosters cooperation among nations, essential for cross-border crime investigations.*																				
CLR-3	*Understanding UNTOC and its role in extradition is crucial for grasping the international legal framework against transnational organized crime. Learners will analyze extradition limitations, principles, and practices, including dual criminality and the rule of speciality. Through case studies and exercises, they'll identify applicable extradition requirements, strategies, and human rights considerations. Additionally, they'll explore bilateral treaties and examine the Revised Manual and Model Law on Extradition, preparing them to navigate complex extradition cases effectively.*																				
CLR-4	*Understanding the challenges faced by prosecuting states in dealing with transnational cybercrimes involves recognizing complexities in evidence gathering across borders and analyzing issues when cybercrimes affect multiple nations. Tutorials and case studies emphasize the importance of international cooperation in cybercrime prosecution, while practices involve researching initiatives like CSCAP and investigating the contributions of organizations like the Digital Opportunity Taskforce of G8.*																				
CLR-5	*Understanding data protection laws like GDPR and CCPA is crucial for cyber forensic investigators to navigate legal requirements. Challenges arise in adhering to these regulations while collecting and handling digital evidence. Ensuring legal compliance maintains the admissibility of evidence in court, highlighting the significance of understanding and adhering to privacy laws.*																				
		Conceive	Design	Implement	Operate	Level of Thinking	Expected Proficiency (%)	Expected Attainment (%)	Disciplinary Knowledge	Critical Thinking	Problem Solving	Analytical Reasoning	Research-related Skills	Communication Skills	Cooperation/Team Work	Digital Literacy	Self-directed Learning	Moral and Ethical Reasoning	Leadership Qualities	Life Long Learning		

Outcomes (CLO)	At the end of this course, learners will be able to:																					
CLO-1	*Upon completion of the course, learners emerge with a deep understanding of jurisdictional complexities and their practical implications. Armed with this knowledge, they can engage in informed discussions and decision-making processes concerning jurisdictional issues in transnational crime cases. Through simulated exercises, mock trials, and research projects, participants apply theoretical knowledge to practical scenarios, honing their ability to assess the jurisdictional competence of courts and legal frameworks in contemporary transnational crime scenarios. Ultimately, graduates contribute to global efforts to combat transnational organized crimes by understanding the role of jurisdiction at the international level and its significance for effective law enforcement and legal cooperation.*	✓	✓		-	2	85	75	3	3	-	1	-	3	-	2	2	1	2	3
CLO-2	*Upon completing the course, learners will adeptly analyze bilateral treaties and UNTOC's role, enhancing their ability to facilitate international cooperation. They will comprehend investigative techniques crucial for transnational crime probes, including crime scene investigation and joint operations. Additionally, they'll evaluate border control measures, ethical implications of surveillance, and proficiency in undercover operations, contributing to comprehensive crime prevention strategies. Practical exercises reinforce theoretical knowledge, ensuring competence in real-world scenarios while reflecting on ethical and legal considerations.*	✓	✓	✓	-	2	85	75	3	-	1	2	2	3	1	1	2	1	2	3
CLO-3	*participants will adeptly apply extradition laws, procedures, and model treaties, ensuring a comprehensive understanding of extradition practices.*	✓	✓	✓	✓	3	85	75	3	1	3	1	3	3	1	1	1	2	1	3
CLO-4	*learners will proficiently identify challenges in prosecuting transnational cybercrimes, assess the impact of cross-border evidence limitations, and understand the significance of awareness among first responders. They will also be capable of evaluating the complexity and cost factors in cybercrime prosecution, emphasizing private sector participation and collaboration between public and private sectors. Practical exercises, including role-playing and recommendation development, enhance their abilities in overcoming jurisdictional hurdles and improving international cooperation mechanisms.*	✓	✓	✓	✓	3	85	75	3	3	2	3	3	2	1	2	3	3	3	3
CLO-5	*learners will possess a comprehensive understanding of data privacy regulations and their implications for cyber forensic investigations. They'll be adept at evaluating challenges faced by investigators, ensuring proper collection techniques, and maintaining evidence integrity. Additionally, learners will develop skills in encryption, decryption, and preserving data integrity in secure environments. They'll be equipped to handle complexities in IoT and cloud forensic analysis and collaborate effectively with cloud service providers to address jurisdictional challenges and maintain chain of custody.*	✓	✓	✓	✓	3	85	75	3	3	2	3	3	3	-	3	3	3	3	3

Strategies					
Technology		Pedagogy / Andragogy		Sustainable Development	
Simulations	✓	Clarification/Pauses	✓	Good Health & Well Being	✓
Presentation Tools					
Learning Management System		Group Discussion	✓	Quality Education	✓
		Hands-on Practice	✓		
		Debate	✓		
		Interactive Lecture	✓		
		Brainstorming	✓		

Designers					
Professional Experts		Higher Institution Experts		Internal Experts	
1	*<name>, <industry name>, <email id>*	1	*<name>, <institution name>, <email id>*	1	*Dr SumanaVedanth.Associate professor, School of Law, SRMIST, <email id>*
2	*<name>, <industry name>, <email id>*	2	*<name>, <institution name>, <email id>*	2	*<name>, SRMIST, <email id>*

Code	PLCS24304T	Title	NATIONAL DEFENCE, TELECOMMUNICATION AND CYBER SECURITY	Category		Professional Elective Courses (E)	L	T	P	C
							3	1	2	5

Course Offering Department	School of Law	Pre-requisite Courses		Co-requisite Courses		Progressive Courses		Data Book / Codes/Standards	

Title & Content	National Defence and cyber security	Organisations and cyber security in India	Telecommunications	E Telecommunication and Broadcasting Sector	Legal Framework
Duration (hour)	18	18	18	18	18
SLO-1	*Define National Security, National Defence, and National Interest - Understand the importance of cyber security in the context of national security - Identify vulnerabilities of information technology and the internet .*	*Understand the landscape of cyber security in India through an analysis of national defense and security issues.*	*Understand the reasons behind vulnerabilities in the telecommunications sector.*	*Understand the regulatory framework governing the telecommunication sector. - Identify key provisions of the Telegraph Act. - Explore the significance of unified license agreements in telecommunications.*	*Understand the significance of legal frameworks in information technology.Analyze the objectives and scope of the Information Technology Act, 2000.*
SLO-2	*Explore different types of cyber security vulnerabilities - Discuss the significance of cyber warfare, including propaganda tactics -*	*Evaluate the role of E-Governance in enhancing cyber security measures.*	*Identify and analyze threats to the telecommunications sector.*	*Examine the vulnerabilities present in telecommunication networks. - Analyze cyber threats and risks associated with telecommunication infrastructure. - Discuss measures to enhance cybersecurity in the telecommunication sector.*	*Interpret the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018. Identify the key components of reasonable security practices and procedures.*
SLO-3	*Analyze the role of social media in shaping national security*	*Analyze the structure and functions of key national organizations such as the National Information Bureau and the National Crisis Management Committee.*	*Examine specific threats such as DDoS attacks, cloud threats, and DNA attacks.*	*Define critical information infrastructure and its importance. - Explore the role of the National Critical Information Infrastructure Protection Centre. - Understand strategies for safeguarding critical information infrastructure.*	*. Define and classify sensitive personal data or information (SPDI) as per the SPDI Rules, 2011. And Explain the role and functions of the Indian Computer Emergency Response Team (CERT-In) under the 2013 rules.*
SLO-4	*Tutorial- Examine real-world examples of cyber attacks and their implications for national security and Discuss strategies for*	*Tutorial- Apply theoretical knowledge to practical scenarios through problem-solving exercises.*	*Tutorial - Case studies and group discussions on real-world telecommunications vulnerabilities and their implications.*	*Tutorial - Review key legal requirements outlined in telecommunication laws.*	*Tutorial - Conduct a legal compliance assessment for an IT organization based on SPDI Rules and Information Technology Act.*

	mitigating cyber threats in various contexts				
SLO-5	*Practical- Conduct hands-on exercises to identify and assess cyber security vulnerabilities - Learn techniques for prioritizing and addressing vulnerabilities effectively*	*Practical - Implement data security measures.*	*Practice:Simulation exercises on mitigating DDoS attacks and securing cloud infrastructure*	*Practice :Review sample unified license agreements used in the telecommunication industry. - Identify clauses and terms within the agreements. - Discuss the implications of unified license agreements on telecommunication services.*	*Practice: Draft a comprehensive security policy adhering to the Information Security Practices and Procedures Rules.*
SLO-6	*Practical-Simulate propaganda campaigns and analyze their impact on national security - Explore countermeasures to combat misinformation and propaganda online*	*Practical- Evaluate the effectiveness of cyber security strategies through case studies and simulations in 2.*	*Practice:Hands-on experience in identifying and securing against internal threats and IoT vulnerabilities.*	*Practice:Evaluate cybersecurity measures implemented in telecommunication networks. - Conduct risk assessments to identify potential vulnerabilities. - Develop strategies to mitigate cybersecurity risks in telecommunication systems.*	*Practice:Develop an incident response plan in accordance with CERT-In guidelines.*
SLO-7	*- Discuss the global reach and rapid dissemination of cyber threats - Examine international laws, regulations, and treaties related to cyber security*	*Understand the role of the Ministry of Home Affairs in addressing security issues .*	*Evaluate regulatory frameworks governing data privacy in telecommunications.*	*Understand the securities issues faced by the telecommunication sector. - Explore the role and functions of the Indian Response Team in addressing security threats. - Discuss strategies for responding to security incidents in telecommunication networks.*	*Explore the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021.*
SLO-8	*Define cyber terrorism and its implications for national security - Study denial of service (DoS) attacks and their potential impact on critical infrastructure*	*Analyze the initiatives and contributions of the Data Security Council of India (DSCI) in enhancing cyber security.*	*Understand the concept of consumer data privacy in telecommunications.*	*Analyze the scope and objectives of DPDP in protecting personal data.*	*Analyze the ethical considerations outlined in the Digital Media Ethics Code.Evaluate the impact of the guidelines on digital media platforms.*
SLO-9	*Analyze the role of government agencies and regulators in ensuring cyber security - Explore best practices for securing government systems and data*	*Critically evaluate the role of the National Cyber Security Co-ordination Centre (NASCCHOM).*	*Analyze state-level infrastructure like SWAN and State Data Centres*	*Explore the role and objectives of the Data Security Council of India. - Understand the initiatives undertaken by DSCI to enhance data security in the telecommunication sector.*	*Understand the objectives and key provisions of the National Cyber Security Policy, 2013.*
SLO-10	*Tutorial- Review existing laws and regulations governing cyber*	*Tutorial -Apply concepts learned in lectures to real-world scenarios.*	*Tutorial-Discuss regulatory guidelines on net neutrality and*	*TutorialIdentify compliance requirements for*	*TutorialDevise a strategy for implementing compliance with the*

	security at national and international levels		*cloud computing.*	*telecommunication companies*	*Guidelines for Intermediaries and Digital Media Ethics Code.*
SLO-11	*Practical- Conduct risk assessments to identify potential cyber threats and their impact on national security*	*Practical - Implement encryption techniques and strategies.*	*Practice-: Hands-on exercises on implementing data privacy measures in telecommunications networks.*	*PracticeEvaluate the effectiveness of response strategies in mitigating security threats.*	*PracticeConduct a compliance audit for a digital media organization, ensuring adherence to the prescribed rules and guidelines.*
SLO-12	*Practice responding to simulated cyber security incidents, including breaches and attacks*	*Practical- Perform vulnerability assessments and risk analysis .*	*Practice: - Case studies on TRAI's initiatives regarding data ownership and security in the telecom sector.*	*Practice: - Identify areas for improvement in data protection practices.*	*Practice: - Perform a risk assessment for an intermediary platform and propose mitigation strategies based on National Cyber Security Policy.*
SLO-13	*Explore cutting-edge technologies and trends in cyber security - Discuss their potential implications for national defense and security strategies*	*Examine the functions and responsibilities of the National Security Council.*	*Explore advanced threats like Vermilion Strike and ShellClient RAT.*	*Define data security and its importance in telecommunication. - Identify common threats to data security in telecommunication networks.*	*Examine the enforcement mechanisms established by the Information Technology Act.and analyze the penalties and consequences for non-compliance with IT regulations.*
SLO-14	*Highlight the importance of cyber security education and awareness programs - Discuss strategies for promoting a culture of cyber security within organizations and society*	*Evaluate the impact and effectiveness of Cyber Threat Intelligence.*	*Examine emerging threats such as LAPUS$ and LightBasin.*	*Review regulatory frameworks governing data security in telecommunication. - Analyze compliance requirements for telecommunication companies.*	*Explore avenues for international cooperation in cybersecurity enforcement. And Analyze the significance of bilateral and multilateral agreements in combating cyber threats.*
SLO-15	*Identify emerging threats and challenges in the field of cyber security*	*Critically analyze the CyberShikshaa initiative and its implications for cyber security.*	*Understand the role of organizations like NASSCOM and DSCI in cybersecurity.*	*Explore the impact of emerging technologies on data security in telecommunication. - Discuss challenges and opportunities presented by technologies such as 5G and IoT.*	*Identify emerging trends in information technology regulation and cybersecurity.And Formulate future strategies for enhancing cybersecurity posture at the national level.*
SLO-16	*Tutorial- Collaboratively develop cyber security policies and guidelines for government and public sector organizations*	*Tutorial - Engage in interactive discussions and problem-solving activities.*	*Tutorial:: Interactive sessions focusing on threat detection and response mechanisms in telecommunications.*	*Tutorial:Discuss the importance of ongoing risk assessment and management in maintaining data security.*	*Tutorial:Simulate a cybersecurity crisis scenario and develop a crisis management plan in alignment with national cybersecurity strategies.*

SLO-17	*Practical -Gain hands-on experience with ethical hacking techniques and penetration testing tools*	*Practical- Implement incident response strategies.*	*Practice:: Simulation exercises on detecting and responding to advanced cyber threats in telecom networks.*	*Practice:Conduct mock compliance audits to assess adherence to data security regulations.*	*Practice:Conduct an incident response simulation exercise to test the effectiveness of response plans and coordination with CERT-In.*
SLO-18	*Practical- Present research projects exploring jurisdictional issues in contemporary transnational crime scenarios.*	*Practical- Develop and implement strategies for enhancing cyber security resilience.*	*Practice:Group exercises on collaborative threat intelligence sharing and response strategies.*	*Practice:Identify challenges and considerations in implementing secure communication protocols in legal scenario through case studies.*	*Practice:Analyze existing IT policies and regulations, and propose recommendations for enhancing their effectiveness and relevance in the evolving digital landscape*

Assessment	*Continuous Learning Assessment - 1*	*Continuous Learning Assessment - 2*
	Continuous Learning Assessment - 3	

Resources			
1	Michael Krausz, The True cost of Information Security Breaches and Cybercrime, 2013, IT Governances Ltd., ISBN:1849284954, ISBN:9781849284950.	7	Michael Krausz, Managing Information Security Breaches, IT Governances Ltd., 2010, ISBN:1849280940, ISBN:9781849280945.
2	Jeremy N.Smith, Breaking and Entering, Eamon Dolan, 2019, ISBN-10:0544903218, ISBN-13:978-0544903210.	8	Michelle Moore, Cyber Security Breaches and Issues Surrounding Online Threat Protection, IGI Global Publications, USA, 2017, ISBN:9781522519416, ISBN:9781522519423 (e-book).
3	Craeme Payne, Equifax Cyber Security Breach 2017, Cybersecurity Executive Advisors LLC, 2019.	9	Scott N.Schober, Cyber Security is Everybody's Business, 2019.
4	William D.Bryant, International Conflict and CyberSpace Superiority, Routledge Publications (2016), ISBN:978-1-138-91891-7(hbk),ISBN:978-1-315-68818-3 (ebk).	10	•KarstenFriis, Conflict in Cyber Space, Routledge Publications (2018).
5	MetodiHadji-Janev, Civil Society and National Security in the Era of Cyber Warfare, IGI Global Publications, Frist Edison (2015), ISBN-13: 978-1466687936, ISBN-10: 1466687932.	11	George Christou, Cybersecurity in the European Union, Palgrave Macmillan (2016), ISBN: 9781137400512.
6	Dr.Kamlesh Bajaj, Cyber Security, Wiley India Publications (2011), ISBN:978-81-265-2179-1, ISBN:978-81-265-8050-7 (ebk).	12	Patrick McCarty, PhD., The Troubled Space of Cyberspace with Senior VP at AnchorFree, insightcommunicationsglobal Publications (2015), ASIN: B014WZWOH0.

Rationale (CLR)	*The purpose of learning this course is to:*
CLR-1	*Learning about national security, defense, and interests entails understanding the vital role of cybersecurity in safeguarding a nation's assets, both physical and digital. It involves recognizing vulnerabilities in information technology and the internet, crucial for protecting critical infrastructure and sensitive data.*
CLR-2	*Understanding the landscape of cyber security in India involves analyzing national defense and security issues, evaluating the role of E-Governance, and understanding the structure and functions of key national organizations. This knowledge aids in comprehending the intricacies of India's cyber security framework.*
CLR-3	*Understanding the vulnerabilities within the telecommunications sector is crucial for professionals aiming to safeguard networks and infrastructure. By delving into the reasons behind these vulnerabilities, individuals can gain insight into potential weaknesses and develop effective strategies to mitigate risks. This course provides a comprehensive understanding of threats such as DDoS attacks and cloud vulnerabilities, enabling participants to identify and analyze potential risks proactively. Through case studies and group discussions, learners engage with real-world scenarios, fostering a deeper understanding of the implications of telecommunications vulnerabilities on both individuals and organizations.*
CLR-4	*Understanding the regulatory framework of the telecommunication sector is crucial for professionals in the field to navigate legal obligations and ensure compliance. By delving into key provisions of acts like the Telegraph Act and grasping the significance of unified license agreements, individuals can operate within legal boundaries and optimize business strategies. Moreover, learning about vulnerabilities in telecommunication networks and cybersecurity measures enhances preparedness against cyber threats, safeguarding both infrastructure and consumer data. Through this course, professionals gain insights into critical information infrastructure protection and strategies to mitigate risks, fostering resilience in an increasingly interconnected digital landscape.*
CLR-5	*The purpose of studying the course on legal frameworks in information technology is to equip individuals with a comprehensive understanding of the legal landscape governing IT. By delving into the Information Technology Act of 2000, learners grasp its objectives and scope, enabling them to interpret the Information Technology (Information Security Practices and Procedures for Protected System) Rules of 2018. Moreover, the course elucidates the classification of sensitive personal data as per the SPDI Rules of 2011 and elucidates the functions of CERT-In. Ultimately, it empowers learners to conduct legal compliance assessments and draft robust security policies for IT organizations.*

Depth	
1	Conceive
2	Design
3	Implement
4	Operate

Attainment	
1	Level of Thinking
2	Expected Proficiency (%)
3	Expected Attainment (%)

Program Learning Outcomes (PLO)	
1	Disciplinary Knowledge
2	Critical Thinking
3	Problem Solving
4	Analytical Reasoning
5	Research-related Skills
6	Communication Skills
7	Cooperation/Team Work
8	Digital Literacy
9	Self-directed Learning
10	Moral and Ethical Reasoning
11	Leadership Qualities
12	Life Long Learning

Outcomes (CLO)	*At the end of this course, learners will be able to:*																							
CLO-1	*learners will be equipped to analyze cyber threats comprehensively, including cyber warfare tactics and the influence of social media on national security. They will gain practical skills through hands-on exercises, such as identifying vulnerabilities and simulating propaganda campaigns. Additionally, learners will explore global cyber threats, cyber terrorism, and governmental roles in cybersecurity, enhancing their ability to contribute to effective cybersecurity strategies and practices.*	✓	✓		-	*2*	*85*	*75*	*3*	*-*	*-*	*1*	*-*	*3*	*-*	*2*	*2*	*1*	*2*	*3*
CLO-2	*learners will be equipped to apply theoretical knowledge to practical scenarios, implement data security measures, and evaluate the effectiveness of cyber security strategies. They will also understand the roles of various national organizations and initiatives such as the Ministry of Home Affairs, Data Security Council of India, and National Cyber Security Co-ordination Centre, contributing to their ability to address cyber security challenges effectively. Additionally, learners will gain hands-on experience in encryption techniques, vulnerability assessments, incident response, and resilience enhancement strategies.*	✓	✓	✓	-	*2*	*85*	*75*	*3*	*2*	*1*	*2*	*2*	*3*	*1*	*1*	*2*	*1*	*2*	*3*
CLO-3	*this course equip individuals with practical skills to address complex threats within the telecommunications sector. Through simulation exercises, participants gain hands-on experience in mitigating DDoS attacks and securing cloud infrastructure, enhancing their ability to implement effective countermeasures. Additionally, the course offers opportunities to evaluate regulatory frameworks governing data privacy and consumer rights, empowering learners to navigate legal complexities confidently. By exploring advanced threats and emerging challenges, such as Vermilion Strike and LAPUS$, professionals develop a proactive approach to cybersecurity. Practical exercises and group discussions facilitate collaboration and the exchange of threat intelligence, preparing individuals to detect and respond effectively to cyber threats in telecom networks.*	✓	✓	✓	✓	*3*	*85*	*75*	*3*	*1*	*3*	*1*	*3*	*3*	*1*	*3*	*3*	*2*	*1*	*3*
CLO-4	*Upon completion of the course, participants acquire a comprehensive understanding of telecommunication sector vulnerabilities and the regulatory framework, empowering them to make informed decisions and implement effective strategies. Analyzing cyber threats and risks equips learners with the ability to identify and mitigate potential breaches, enhancing overall cybersecurity in telecommunication networks. Furthermore, insights into critical information infrastructure and compliance requirements enable professionals to protect sensitive data and infrastructure effectively. With a focus on practical exercises such as reviewing sample license agreements and evaluating cybersecurity measures, participants develop practical skills to address security issues and enhance data protection practices, ensuring resilience in the face of evolving threats.*	✓	✓	✓	✓	*3*	*85*	*75*	*3*	*3*	*2*	*3*	*3*	*3*	*1*	*2*	*3*	*3*	*3*	*3*
CLO-5	*Through this course, learners gain insight into the multifaceted learning outcomes. They develop analytical skills to assess legal frameworks and understand the nuances of IT regulations. By drafting security policies and incident response plans, they enhance practical competencies in compliance management. Moreover, they grasp ethical considerations in digital media outlined in the Ethics Code and evaluate their impact on digital platforms. Understanding the National Cyber Security Policy aids in strategizing compliance implementation. Additionally, learners simulate crisis scenarios, honing crisis management skills and proposing future strategies to bolster national cybersecurity. This course fosters a holistic understanding of IT law, cybersecurity, and ethical implications in the digital sphere.*	✓	✓	✓	✓	*3*	*85*	*75*	*3*	*3*	*2*	*3*	*3*	*3*	*-*	*3*	*3*	*3*	*3*	*3*

Strategies					
Technology		Pedagogy / Andragogy		Sustainable Development	
Simulations	✓	Clarification/Pauses	✓	Good Health & Well Being	✓
Presentation Tools					
Learning Management System		Group Discussion	✓	Quality Education	✓
		Hands-on Practice	✓		
		Debate	✓		
		Interactive Lecture	✓		
		Brainstorming	✓		

Designers					
Professional Experts		Higher Institution Experts		Internal Experts	
1	*<name>, <industry name>, <email id>*	1	*<name>, <institution name>, <email id>*	1	*Anand Shukla, Assistant Professor, School of Law, , SRMIST, <email id>*
2	*<name>, <industry name>, <email id>*	2	*<name>, <institution name>, <email id>*	2	*<name>, SRMIST, <email id>*

Code	PLCS24305T	Title	INTELLECTUAL PROPERTY RIGHTS AND CYBER SECURITY	Category		Professional Core (Elective)	L	T	P	C
							3	1	2	5

Course Offering Department	School of Law	Pre-requisite Courses	IPR	Co-requisite Courses	Nil	Progressive Courses	Nil	Data Book / Codes/Standards	

Title & Content	Unit 1	Unit 2	Unit 3	Unit 4	Unit 5
Duration (hour)	18	18	18	18	
SLO-1	Analyze the fundamental concepts of property and intellectual property, considering their philosophical underpinnings and impacts on legal systems, societal norms, and economies.	Evaluate the intricacies of copyright law in both traditional and digital environments, scrutinizing the roles of rights holders and the challenges posed by private use and fair use doctrines in digital information dissemination.	Critically evaluate the intersection of trademarks and domain names, examining challenges and opportunities in their use as internet addresses..	Assess the impact of cyber security on patenting, analyzing challenges and opportunities presented by the internet era.	Evaluate the importance of biodiversity and its role in ecosystems, emphasizing its relevance in the digital age.
SLO-2	Evaluate the historical development and modern significance of intellectual property rights, incorporating diverse viewpoints to understand their role in fostering innovation, creativity, and cultural expression.	Critically assess key international agreements such as the Berne Convention, TRIPS Agreement, WIPO Copyright Treaty (WCT), and WIPO Performances and Phonograms Treaty (WPPT), elucidating their significance in harmonizing copyright laws globally	Assess legal protections under competition law and tort law against unauthorized use of similar domain names, considering implications for trademark holders.	Critically examine the phenomena of patent thickets and patent trolls, exploring their implications for innovation and competition in the digital landscape.	Differentiate between patents, trademarks, copyrights, trade secrets, Geographic Indications (GIs), and design rights in the context of biodiversity conservation.
SLO-3	Assess the connection between intellectual property rights and human rights, using advanced theories to explore issues of fairness, accessibility, and ethical concerns in a globalized knowledge-based society.	Analyze the provisions of the Indian Copyright Act, 1957 and its subsequent amendments, comprehending the nuances of copyright works, ownership, transfer, duration, renewal, termination, and remedies for infringement under Indian legal framework..	Evaluate international regulations governing domain names, including the roles of organizations like the International Telecommunications Union and the International Trademark Association.	Investigate the intersection of patent law and privacy concerns in the internet age, discerning potential conflicts and regulatory gaps.	Explore how GIs and design rights contribute to safeguarding biodiversity-related products and innovations.

SLO-4	**Tutorial:** Define intellectual property and its significance. Research its historical evolution to understand its importance in various domains.	**Tutorial:** Analyze case studies illustrating copyright challenges in digital environments.	**Tutorial :** Analyze case studies of trademark disputes involving domain names and discuss relevant legal principles**.**	**Tutorial:** Analyze case studies of cyber security-related patents and discuss their implications for innovation and security.	**Tutorial:** Analyze case studies highlighting the impact of biodiversity loss.
SLO-5	**Practice:** Analyze the conceptual framework, historical trajectory, and various types of intellectual property, including their emergence as human rights.	**Practice**: Group discussion and idea generation on the complexities of copyright protection and enforcement..	**Practice:** Brainstorm potential trademark conflicts and legal considerations in domain name use**.**	**Practice:** Break into groups, review assigned case studies, and propose solutions for addressing patent thicket and troll issues.	**Practice:** Identify and classify various forms of IP rights associated with biodiversity-related products and innovations.
SLO-6	**Practice:** Conduct a Group Discussion to Explore the influence of international institutions on intellectual property regulation and strategies for commercialization through licensing agreements.	**Practice:** Break into groups, analyze assigned case studies, and discuss potential solutions and legal remedies.	**Practice:** Break into groups, analyze assigned case studies, and propose resolutions to domain name conflicts**.**	**Practice:** Brainstorm potential challenges and share insights on patenting strategies in the digital landscape.	**Practice:** Analyze case studies and examples to understand how Geographic Indications (GIs) and design rights contribute to biodiversity conservation and IP protection.
SLO-7	Examine international regulatory frameworks for intellectual property, critically analyzing their effectiveness, limitations, and implications for worldwide commerce and development.	Critique the role of business models in safeguarding intellectual property rights, exploring innovative strategies employed by businesses to protect copyrighted works in various sectors.	Understand the complexities of trademark disputes arising from the use of domain names, including policies for internet domain registration and resolution mechanisms.	Explore the complexities of patents and personal data protection, considering legal frameworks and ethical considerations in data-driven innovation.	Investigate lesser-known forms of IP protection and their impact on biodiversity conservation efforts.
SLO-8	Develop effective strategies for commercializing intellectual property through licensing agreements, drawing on expertise from legal, economic, and strategic management fields to maximize value and minimize risks.	Analyze the legal liabilities associated with online copyright infringement, examining the responsibilities of internet service providers, content platforms, and users in the digital ecosystem.	Explore strategies for protecting trademarks and commercial designations against unauthorized use in domain names, including legal and technological approaches.	Examine the legal and practical aspects of software patents and mobile app patents, understanding their role in technology innovation and commercialization.	Analyze the interconnectedness of biodiversity, IP, and cyber law, focusing on challenges posed by cyber security threats to biodiversity data and IP assets.
SLO-9	Apply advanced financial modeling techniques to determine the value of intellectual property rights, considering market dynamics, technological advancements,	Interpret the complexities of copyright ownership, transfer, and duration, examining legal frameworks governing the acquisition, assignment, licensing, and termination of	Analyze the implications of using domain names as internet addresses by companies in different sectors of business, considering trademark conflicts and consumer confusion.	Analyze the governance mechanisms governing the internet and their implications for intellectual property rights enforcement and protection.	Discuss ethical considerations in biodiversity conservation, IP protection, and cyber security, considering the implications of emerging technologies.

	and legal precedents for informed decision making	copyright.			
SLO-10	**Tutorial:** Investigate international regulatory frameworks governing intellectual property. Learn financial valuation techniques and negotiation strategies for commercializing intellectual property rights.	**Tutorial** : Conduct a comparative analysis of Indian copyright law with international treaties.	**Tutorial** - Research and present on the roles of international organizations in regulating domain name use.	**Tutorial:** Conduct a comparative analysis of patent thicket and troll cases and propose strategies for mitigating their negative effects.	**Tutorial:** Evaluate the effectiveness of Geographic Indications (GIs) and design rights in safeguarding biodiversity-related products.
SLO-11	**Practice**: Learn financial valuation methods for intellectual property rights and develop negotiation skills for determining payment terms in transactions.	**Practice:** Divide participants into teams, assign positions, and debate the merits and limitations of fair use doctrines.	**Practice:** Collaboratively develop trademark protection plans, discuss best practices, and share insights on trademark enforcement.	**Practice:** Collaboratively develop patent protection plans and discuss best practices for patenting internet technologies**.**	**Practice:** Evaluate existing policy frameworks related to biodiversity conservation, IP protection, and cyber security, and propose recommendations for improvement.
SLO-12	**Practice**: Learners explore jurisdictional nuances in intellectual property rights (IPR) cases in cyber space, examining legal decisions and comparing approaches in different jurisdictions.	**Practice**: Interactive session covering topics such as licensing, permissions, and copyright infringement prevention measures..	**Practice:** Assign roles such as trademark holder, domain name registrant, and mediator, and engage in negotiations to reach a resolution.	**Practice:** Divide participants into teams, assign positions, and debate the ethical and legal implications of software patents**.**	**Practice:** Engage in discussions on ethical dilemmas concerning biodiversity conservation, IP protection, and cyber security, and propose ethical solutions.
SLO-13	Formulate sophisticated negotiation tactics for intellectual property transactions, utilizing principles from contract law, negotiation theory, and intellectual property jurisprudence to achieve favorable outcomes and prevent conflicts.	Discriminate between acts constituting copyright infringement and explore available legal remedies, including injunctions, damages, and statutory damages, to protect copyrighted works against unauthorized use.	Examine conflicts arising from international domain name use and explore mechanisms for resolving disputes, including the role of international committees and organizations.	Critique patenting strategies for social media platforms, evaluating their effectiveness in protecting intellectual property rights in digital content dissemination.	Assess policy frameworks governing biodiversity conservation, IP protection, and cyber security, considering their effectiveness in addressing current challenges.
SLO-14	Evaluate the impact of digital technologies on intellectual property rights, exploring challenges and opportunities posed by online platforms and decentralized networks for traditional legal frameworks and business strategies.	Investigate the challenges posed by wide-ranging private use copying and fair use doctrines in digital environments, analyzing their implications on copyright holders and content consumers.	Understand the relationship between patents, geographical indications, and domain names, considering their implications for intellectual property rights.	Analyze patenting trends in internet technologies, identifying emerging areas of innovation and potential legal challenges.	Examine case studies illustrating real-world challenges and solutions in managing biodiversity, protecting IP assets, and addressing cyber security threats.

SLO-15	Synthesize interdisciplinary perspectives to propose innovative solutions for complex intellectual property issues, using critical thinking, ethical analysis, and strategic foresight to address the dynamic tensions between innovation, regulation, and societal well-being in a knowledge-driven economy.	Apply acquired copyright knowledge to practical scenarios, devising strategies for effective copyright protection and enforcement in diverse contexts such as creative industries, digital platforms, and online marketplaces.	Explore the concept of domain names as catchwords and their significance in branding and marketing strategies, considering their impact on consumer recognition and brand identity.	Develop strategies for patent protection in the digital age, considering legal, technological, and business factors in safeguarding intellectual property rights	Explore emerging technologies shaping the landscape of biodiversity conservation, IP protection, and cyber security, and their potential impact on sustainable management practices.
SLO-16	**Tutorial**: Develop strategies for implementing and integrating digital solutions into intellectual property management practices, considering factors such as cost, scalability, and compatibility with existing systems	**Tutorial**: Develop innovative business strategies for copyright protection and monetization.	**Tutorial:** Develop a trademark protection plan for a hypothetical company facing domain name disputes.	**Tutorial :** Explore case studies of landmark software and mobile app patent cases and discuss their impact on industry practices.	**Tutorial:** Develop strategies to mitigate cyber security risks through case study analysis and policy discussions.
SLO-17	**Practice**: Examine real-world cases of intellectual property management, applying theoretical knowledge to practical scenarios and deriving insights for effective decision-making.	**Practice**: Assign roles to participants (e.g., plaintiff, defendant, legal counsel) and conduct a simulated trial with arguments and evidence presentation..	**Practice:** Divide participants into teams, assign positions, and debate the merits and drawbacks of different domain name policies.	**Practice:** Assign roles such as cyber security experts, patent attorneys, and patent trolls, and engage in negotiations to protect intellectual property rights.	**Practice:** Simulate cyber security threats targeting biodiversity data and IP assets, and develop strategies to mitigate risks.
SLO-18	**Practice**: Collaborate to develop strategic plans for navigating the complexities of intellectual property rights, considering legal, economic, and ethical dimensions in a globalized context.	**Practice:** Collaborative workshop on topics such as digital rights management, content protection technologies, and copyright enforcement tactics.	**Practice:** Share experiences, tips, and strategies for effective domain name management, and discuss case studies of successful domain name campaigns.	**Practice:** Discuss case studies of successful mobile app patents and brainstorm innovative patenting strategies for mobile app developers.	**Practice:** Research and present on emerging technologies influencing biodiversity conservation, IP protection, and cyber security, and discuss their potential implications**.**

Assessment	*Continuous Learning Assessment - 1*	*Continuous Learning Assessment - 2*
	Continuous Learning Assessment - 3	

Resources			
1	The Copyright Act, 1957	6	Rajesh Singh, Unfolding Intellectual Property Rights, Notion Publications (2019), ISBN:978-1-64546-536-2 (e-book).
2	The Patent Act, 1970	7	S. Racherla, Innovation, Economic Development, and Intellectual Property in India and China, Springer Publications (2019), ISBN:978-981-13-8101-0 (e-book), ISBN:978-981-13-8102-7.
3	Raymond J.Hegarty, Billion Dollar Strategy, (2019)	8	Land Mark Publications (2011), Cyber Law
4	Vikas Vashishth.; “Law and practice of intellectual property in India”Sreenivasulu N.S; “Law Relating to Intellectual Property”, Patridge Publishing, 2013.	9	Vakul Sharma; “Information Technology: Law and Practice”, Universal Law Publishing Co., India, 2011
5	Biodiversity Act 2002	10	Geographical Indication Act 1999

Rationale (CLR)	The purpose of learning this course is to:	Depth				Attainment			Program Learning Outcomes (PLO)												
		1	2	3	4	1	2	3	1	2	3	4	5	6	7	8	9	10	11	12
CLR-1	Developing a comprehensive understanding of property and intellectual property, covering conceptual foundations, historical evolution, international aspects, commercialization strategies, financial valuation methods, negotiation skills, and digital domain impact, equips students to navigate legal and economic landscapes effectively, ensuring proficient asset protection, management, and utilization.																				
CLR-2	Develop a comprehensive understanding of copyright principles, encompassing its application in digital environments, rights management, international treaties, Indian copyright law, and infringement remedies, equips students with the capacity to navigate complex legal frameworks and protect intellectual property rights effectively in the digital era.																				
CLR-3	Mastery in analyzing trademark concepts, particularly their application to domain names, equips students to adeptly navigate international regulations and formulate comprehensive policies for internet domain registration, ensuring robust protection of intellectual property rights in the digital realm.																				
CLR-4	Demonstrating advanced proficiency in scrutinizing the multifaceted intersections between patent law and cybersecurity enables students to comprehend contemporary digital challenges, including patent thickets and privacy concerns, and grasp their broader implications on internet governance and intellectual property rights.																				
CLR-5	Analyze the intricate relationships among biodiversity, Intellectual Property (IP), and cyber law, empowering them to navigate intricate challenges presented by cyber security threats and make substantial contributions to the sustainable management of biodiversity and intellectual assets in the digital era.																				
Outcomes (CLO)	At the end of this course, learners will be able to:	Conceive	Design	Implement	Operate	Level of Thinking	Expected Proficiency (%)	Expected Attainment (%)	Disciplinary Knowledge	Critical Thinking	Problem Solving	Analytical Reasoning	Research-related Skills	Communication Skills	Cooperation/Team Work	Digital Literacy	Self-directed Learning	Moral and Ethical Reasoning	Leadership Qualities	Life Long Learning
CLO-1	Comprehensive understanding of property and intellectual property, including their conceptual foundations, historical evolution, international aspects, commercialization strategies, financial valuation methods, negotiation skills, and the impact of intellectual property rights in the digital domain.	✓	✓		-	2	85	75	3	-	-	1	-	3	-	2	2	1	2	3
CLO-2	Develop a comprehensive understanding of copyright principles, encompassing its application in digital environments, rights management, international treaties, Indian copyright law, and infringement remedies.	✓	✓	✓	-	2	85	75	3	2	1	2	2	3	-	1	2	1	2	3
CLO-3	Proficiently analyze trademark concepts, including their application to domain names, navigate international regulations, and formulate policies for internet domain registration.	✓	✓	✓	✓	3	85	75	3	1	3	1	3	3	-	1	1	2	1	3
CLO-4	Demonstrate advanced proficiency in analyzing the multifaceted intersections between patent law and cybersecurity, including challenges within the digital era, such as patent thicket and trolls, as well as navigating complexities surrounding privacy concerns, personal data, software patents, mobile applications, social media, and their implications on internet governance and intellectual property rights.	✓	✓	✓	✓	3	85	75	3	3	2	3	3	3	-	2	3	3	3	3
CLO-5	Analyze the interconnectedness of biodiversity, Intellectual Property (IP), and cyber law in the modern digital age, enabling them to navigate complex challenges posed by cyber security threats and contribute significantly to the sustainable management of biodiversity and intellectual assets.								3	2	2	2	3	2	1	3	3	3	2	3

Assessment Method (Max. Marks: 100)																			
		Continuous Learning Assessment (CLA 40% Weightage)												Final Exam					
Level of Thinking		Model Exam (20%)				Assignment/ Seminar/Group discussion/ Presentation				Participation in seminar/ Conference/ Publication				Participation in class room/co-curricular & Para curricular activities					
		(20%)				(10%)				(5%)				(5%)				(60%)	
1	Remember	40%		-		40%		-		30%		-				-		40%	-
2	Understand																		
3	Apply	40%		-		40%		-		40%		-				-		40%	-
4	Analyze																		
5	Evaluate	20%		-		20%		-		30%		-				-		20%	-
6	Create																		
Total		100 %				100 %				100 %				100 %				100 %	

Strategies					
Technology		Pedagogy / Andragogy		Sustainable Development	
Simulations	✓	Clarification/Pauses	✓	Good Health & Well Being	✓
Presentation Tools					
Learning Management System		Group Discussion	✓	Quality Education	✓
		Hands-on Practice	✓		
		Debate	✓		
		Interactive Lecture	✓		
		Brainstorming	✓		

Designers					
Professional Experts		Higher Institution Experts		Internal Experts	
1	<name>, <industry name>, <email id>	1	<name>, <institution name>, <email id>	1	<name>, SRMIST, <email id>
2	<name>, <industry name>, <email id>	2	<name>, <institution name>, <email id>	2	<name>, SRMIST, <email id>

MINI PROJECT CORE PRACTICAL

Code	PLCS24306P	Title	MINI PROJECT	Category	Core Practical (P)	L	T	P	C
						0	1	4	3

Course Nature: Practical					
Assessment Method (Max Marks:100)					
End-semester	Assessment Tools	Written- Submission	Presentation	Viva Voce	Total
	Marks	60	20	20	100
				Total Max Marks	100

Code	PLCS24401T	Title	CRYPTO CURRENCY AND LEGAL ISSUES	Category		Professional Core (Elective)	L	T	P	C
							3	1	2	5

Course Offering Department	School of Law	Pre-requisite Courses	Nil	Co-requisite Courses	Nil	Progressive Courses	Nil	Data Book / Codes/Standards	

Title & Content	Unit 1	Unit 2	Unit 3	Unit 4	Unit 5
Duration (hour)	18	18	18	18	18
SLO-1	Evaluate the foundational concepts and definitions of cryptography, distinguishing between symmetric and asymmetric cryptosystems.	Assess and define key cryptocurrency terminology to facilitate a comprehensive understanding.	Evaluate the mechanism through which Bitcoin achieves decentralization, including the role of miners, nodes, and the blockchain.	Analyze the process of purchasing Bitcoins through platforms like Coinigy, including understanding the steps involved and associated risks.	Analyze research perspectives and challenges within the Bitcoin ecosystem, exploring scalability issues, regulatory hurdles, and technological advancements.
SLO-2	Implement classical encryption methods including substitution techniques, transposition techniques, and analyze their strengths and weaknesses.	Evaluate various practical applications and potential uses of cryptocurrency within financial and non-financial domains.	Analyze the mechanics of Bitcoin transactions, including the process of mining, verifying transactions, and adding blocks to the blockchain..	Evaluate the main approaches utilized by Coinigy, with a focus on Coin predictions, market fundamentals, and technical analysis techniques.	Evaluate the integration of Bitcoins in contracts and wallets, understanding their legal implications, security considerations, and practical applications.
SLO-3	Differentiate between block ciphers and stream ciphers, and assess their suitability for various cryptographic applications.	Demonstrate proficiency in explaining the foundational principles and mechanics of blockchain technology.	Demonstrate how to securely store and utilize Bitcoin, including the use of wallets, private keys, and best practices for transaction security.	Apply Dow theory principles to analyze market indices and assess the state of the cryptocurrency market, particularly focusing on Bitcoin.	**Assess** the usability of Bitcoins in foreign countries and India, considering factors such as regulatory environment, infrastructure, and cultural acceptance.
SLO-4	**Tutorial:** Implement classical encryption techniques like substitution and transposition.	Tutorial: Analyze cases, compare regulations, and develop compliance strategies for cross-border e-commerce, culminating in group presentations.	**Tutorial :** Deconstruct the concept of Bitcoin's decentralization, examining the roles of miners and nodes through interactive simulations and discussions.	**Tutorial** : Navigate the Coinigy platform to understand its interface and functionalities.	Tutorial : Explore scalability issues, regulatory hurdles, and technological advancements shaping the future of Bitcoin.
SLO-5	**Practice:** Implement substitution and transposition techniques on sample plaintexts, and analyze the effectiveness of each method.	**Practice:** Define and match key cryptocurrency terms to their respective definitions through an interactive quiz format.	**Practice:** Participate in a simulated exercise to execute Bitcoin transactions, emphasizing security measures and privacy considerations.	Practice: Participate in a simulated exercise using the Coinigy platform to practice purchasing Bitcoins and navigating the cryptocurrency market.	Practice: Engage in a simulation exercise to create and execute Bitcoin contracts, while practicing wallet management and security protocols.

SLO-6	**Practice:** Compare and contrast block ciphers and stream ciphers, and assess their performance in encrypting data streams of varying lengths.	**Practice**: Semulate a blockchain transaction to understand its underlying technology and operational processes..	**Practice:** Engage in a debate forum discussing community politics and regulation within the Bitcoin ecosystem, exploring various perspectives and proposed solutions.	Practice: Engage in a workshop focused on technical analysis techniques used in cryptocurrency trading, with hands-on exercises using Coinigy.	Practice: Participate in a workshop to explore the usability of Bitcoins in foreign countries and India, conducting practical exercises and case studies.
SLO-7	Develop an understanding of hybrid encryption methods, integrating both symmetric and asymmetric encryption for enhanced security.	Analyze the legal implications of cryptocurrencies in international and public law, focusing on monetary concepts and regulatory challenges.	Evaluate the level of anonymity provided by Bitcoin transactions and the potential risks associated with privacy concerns.	Analyze the application of Bitcoin and other cryptocurrencies, including their introduction to cryptography and the underlying technologies.	Examine Bitcoin mining strategy attacks, including 51% attacks, double-spending attacks, and selfish mining, and their impact on network security and decentralization.
SLO-8	Understand the principles of the one-time pad encryption technique and its implications for information security.	Assess and propose effective regulatory frameworks for cryptocurrencies and other forms of value data.	Utilize the role of community politics in the regulation and governance of Bitcoin, including debates over scalability, protocol upgrades, and regulatory compliance.	Interpret the Nakamoto Consensus and Bitcoin white paper to understand the foundational concepts of Bitcoin protocols.	Explore the economics and politics of the Bitcoin community, including governance models, decision-making processes, and ideological debates.
SLO-9	Assess security measures for email communication and internet browsing, identifying vulnerabilities and countermeasures	Critically evaluate legal conflicts arising from cryptocurrencies across different jurisdictions and legal systems.	Compare alternative mining puzzles utilized by Bitcoin, such as Proof of Work (PoW) and Proof of Stake (PoS), and their impact on decentralization and energy consumption.	Explore research perspectives and challenges within the Bitcoin ecosystem, including scalability issues and protocol improvements.	Compare and contrast altcoins, providing an overview of their features, use cases, and market dynamics, and analyzing their potential impact on the cryptocurrency ecosystem.
SLO-10	**Tutorial:** Investigate email, internet, and web security protocols..	Tutorial : Assign scenarios, have students draft e-commerce contracts, engage in peer review, and facilitate class discussion on challenges and revisions.	Tutorial – Engage in a hands-on workshop to practice secure Bitcoin usage, including setting up wallets, executing transactions, and implementing best practices for privacy and security.	Tutorial – Apply technical analysis techniques on Coinigy to analyze market trends and predict price movements.	Tutorial – Conduct a legal analysis of Ethereum contracts, discussing their enforceability and regulatory compliance.
SLO-11	**Practice:** Design a hybrid encryption scheme incorporating both symmetric and asymmetric encryption, and evaluate its effectiveness in securing sensitive data.	**Practice**: Analyze existing regulatory frameworks for cryptocurrencies and propose revisions or enhancements to address emerging challenges.	Practice: Conduct a workshop comparing different mining puzzles used by Bitcoin and alternative cryptocurrencies, analyzing their pros and cons.	Practice: Join a debate forum to discuss and analyze current market trends in cryptocurrencies, utilizing Coinigy data for insights.	Practice: Analyze various Bitcoin mining strategies and potential attack vectors, discussing countermeasures and risk mitigation techniques.
SLO-12	**Practice:** Conceal a message within an image using steganography techniques, and	**Practice:** Discuss and analyze real-world legal cases involving disputes related to cryptocurrency	Practice: Collaborate on a project to analyze the market dynamics and ecosystem of selected	Practice: Participate in a simulation exercise where students invest virtual currency	Practice: Engage in a debate forum discussing the economics and politics of the Bitcoin

	develop methods for detecting hidden data.	ownership or transactions.	Altcoins, presenting findings and recommendations for investment strategies.	using Coinigy's analysis platform, applying learned approaches and theories.	community, considering different perspectives and ideologies.
SLO-13	Investigate steganography techniques for hiding data within digital media and employ methods for detecting concealed information.	Analyze and compare the treatment of cryptocurrencies as property in common law and civilian legal systems.	Examine Bitcoin as a platform for innovation and development, including the creation of smart contracts, decentralized applications (DApps), and tokenization.	Identify common issues and solutions outlined in the Bitcoin developer guide, focusing on best practices for blockchain transactions.	Analyze Ethereum's overview, including its features, smart contract capabilities, and its role in blockchain innovation.
SLO-14	Evaluate the Data Encryption Standard (DES) algorithm, understanding its design principles and cryptographic properties.	Investigate and compare the legal characterization and regulation of cryptocurrencies in East Asian jurisdictions.	Analyze the ecosystem of alternative coins (Altcoins) and other cryptocurrencies, considering their unique features, use cases, and market dynamics.	Analyze the functioning of blockchain transactions within a peer-to-peer network, understanding the security and transparency mechanisms involved.	Evaluate the legal implications of Ethereum contracts, including their enforceability, regulatory compliance, and potential impact on traditional legal frameworks.
SLO-15	Examine the principles underlying public key cryptosystems, focusing on the RSA algorithm and key management strategies, including Diffie-Hellman Key Exchange.	Engage in critical analysis of legal conceptions of cryptocurrencies, including their status as property and their implications in economic systems.	Evaluate the intersection of Bitcoin and traditional banking systems, exploring challenges, opportunities, and regulatory responses.	Synthesize knowledge of Coinigy's analysis platform, Bitcoin fundamentals, and blockchain technology to make informed decisions in cryptocurrency trading and investment.	Conduct a case study analysis of Ethereum, examining real-world applications, challenges faced, and lessons learned.
SLO-16	**Tutorial:** Explore RSA algorithm and key management, including Diffie-Hellman Key Exchange.	Tutorial : Simulate an e-commerce dispute, assign roles (lawyers, mediators), and engage in negotiation, mediation, or arbitration, followed by a debrief and analysis.	Tutorial : Participate in a regulatory roundtable discussion to understand Bitcoin's legal landscape, followed by an exploration of emerging trends in the cryptocurrency market and their potential implications.	Tutorial : Engage in discussions on the challenges and research perspectives in Bitcoin protocols, and explore potential solutions and advancements.	Tutorial : Discuss Bitcoin mining strategy attacks and their impact on network security, exploring countermeasures and risk mitigation techniques.
SLO-17	**Practice:** Analyze the structure and operation of the Data Encryption Standard (DES), and assess its security strengths and weaknesses.	**Practice:** Participate in a structured debate exploring diverse perspectives on the regulation of cryptocurrencies, considering both advantages and disadvantages of various approaches.	Practice: Attend a panel discussion featuring experts from the cryptocurrency and banking sectors, exploring the evolving relationship between Bitcoin and traditional banking systems.	Practice: Conduct experiments in a lab setting to understand the mechanics of blockchain transactions and peer-to-peer networks, using Bitcoin as a case study.	Practice: Collaborate on a project to research and analyze selected altcoins, presenting findings on their features, use cases, and market trends.

SLO-18	**Practice:** Implement the RSA algorithm for key generation and encryption, and explore key management strategies, including the Diffie-Hellman Key Exchange protocol.	**Practice:** Compare and contrast the legal treatment and regulatory approaches to cryptocurrencies across different East Asian jurisdictions.	Practice: Participate in an exercise to identify and assess operational risks related to cybersecurity, accounting, and anti-money laundering issues within the Bitcoin ecosystem.	Practice: Collaborate on a research project exploring various perspectives and challenges within Bitcoin protocols, presenting findings to the class for discussion and analysis.	Practice: Attend a symposium exploring blockchain innovations, including pegged sidechains, and their potential applications in various industries, discussing future trends and challenges with industry experts.
Assessment	Continuous Learning Assessment - 1		Continuous Learning Assessment - 2		
	Continuous Learning Assessment - 3				

Resources			
1	Christian Newman, BitcoinFrom Beginner to Export, Kobo Publications, 2019, ISBN-13:9781518987892, ISBN-10: 1518987893.	6	Michael Scott, BitcoinFor Beginners, Kobo Publications, 2019, ISBN-13: 9781518996535, ISBN-10: 1518996531.
2	Matteo Le Riche, Bitcoin, CreateSpace Independent Publishing Platform, 2017, ISBN 10: 1975920414/ ISBN 13: 9781975920418.	7	Anthony TU, Crypto Currency for Beginners, Career Publications, 2017, ISBN-10 : 1976158877 ISBN-13 : 9781976158872.
3	Christian Newman, Crypto Currency Investing Ultimate Guide, Book Zone Publications, ISBN:9781980244547	8	Samuel Rees, Bitcoin, Samuel Rees Publications, 2017, ASIN: B077NBZ7D2
4	Chris Lambert,Investing in Crypto currency, Amazon Asia-Pacific Holdings Private Limited, ASIN: B073SH7MMX, Kindle Edition	9	Cryptocurrencies in Public and Private Law, David Fox and Sarah Green, ISBN: 9780198826385
5	Arvind Narayanan, Bitcoin and Cryptocurrency technologies, Princeton University Press, 2016 Publications, ISBN - 9780691171692	10	Charles Hamilton, The Ultimate Guide to Crypto Currencies and Digital Money.

Rationale (CLR)	The purpose of learning this course is to:	Depth				Attainment			Program Learning Outcomes (PLO)												
		1	2	3	4	1	2	3	1	2	3	4	5	6	7	8	9	10	11	12
CLR-1	Equip students with a comprehensive understanding of cryptography fundamentals, covering various encryption techniques, security protocols, and key management strategies essential for navigating modern cryptographic systems.																			
CLR-2	Comprehensive exploration of cryptocurrency, covering its terminology, applications, blockchain technology, monetary nature, legal implications, regulatory frameworks, legal treatment, and regional characterizations, fostering a deep understanding of its multifaceted nature and significance in the global context.																			
CLR-3	Facilitate a thorough examination of various aspects surrounding Bitcoin, including its decentralization, storage, usage, regulatory landscape, alternative cryptocurrencies, banking relationships, taxation implications, and cybersecurity concerns, providing students with a comprehensive understanding of its multifaceted nature and associated risks.																			
CLR-4	Equip students with the ability to navigate the purchase of Bitcoins using Coinigy, involving analyzing its platform, exploring various market prediction strategies, and contextualizing the application of cryptocurrencies, such as Bitcoin, within the realms of cryptography and blockchain technology.																			
CLR-5	Enable students to critically assess the incorporation of Bitcoin into contracts and wallets, evaluating their legal ramifications, security concerns, and real-world utility.																			

Outcomes (CLO)	At the end of this course, learners will be able to:	Conceive	Design	Implement	Operate	Level of Thinking	Expected Proficiency (%)	Expected Attainment (%)	Disciplinary Knowledge	Critical Thinking	Problem Solving	Analytical Reasoning	Research-related Skills	Communication Skills	Cooperation/Team Work	Digital Literacy	Self-directed Learning	Moral and Ethical Reasoning	Leadership Qualities	Life Long Learning
CLO-1	Examine the basics of cryptography, including definitions, symmetric and asymmetric cryptosystems, classical encryption techniques, email and web security, steganography, Data Encryption Standard (DES), public key cryptosystems like RSA, and key management including Diffie-Hellman Key Exchange.	✓	✓		-	2	85	75	3	-	-	1	-	3	-	2	2	1	2	3
CLO-2	Investigate the world of cryptocurrency, encompassing fundamental terminology, diverse applications, the underlying technology of blockchain, its virtual monetary nature, implications in international and public law, regulatory frameworks, conflicts of laws, treatment within common law and civil legal systems, and characterizations in East Asia.	✓	✓	✓	-	2	85	75	3	2	1	2	2	3	-	1	2	1	2	3
CLO-3	Explore Bitcoin's decentralization mechanisms, mechanics, storage and usage methods, anonymity, community politics, regulations, mining puzzles, platform aspects, altcoins, banking connections, taxation, non-state virtual currencies, and cybersecurity and operational risks.	✓	✓	✓	✓	3	85	75	3	1	3	1	3	3	-	1	1	2	1	3
CLO-4	Explore the purchase of Bitcoins through Coinigy, delving into its analysis platform, main approaches, market prediction strategies, and the application of cryptocurrencies, including Bitcoin, within the context of cryptography and blockchain technology.	✓	✓	✓	✓	3	85	75	3	3	2	3	3	3	-	2	3	3	3	3
CLO-5	Analyze the integration of Bitcoin in contracts and wallets, assessing their legal implications, security considerations, and practical applications.	✓	✓	✓	✓	3	85	75	3	3	2	3	3	3	-	3	3	3	3	3

Assessment Method (Max. Marks: 100)																			
		Continuous Learning Assessment (CLA 40% Weightage)												Final Exam					
Level of Thinking		Model Exam (20%)				Assignment/ Seminar/Group discussion/ Presentation				Participation in seminar/ Conference/ Publication				Participation in class room/co-curricular & Para curricular activities					
		(20%)				(10%)				(5%)				(5%)				(60%)	
1	Remember	40%		-		40%		-		30%		-				-		40%	-
2	Understand																		
3	Apply	40%		-		40%		-		40%		-				-		40%	-
4	Analyze																		
5	Evaluate	20%		-		20%		-		30%		-				-		20%	-
6	Create																		
Total		100 %				100 %				100 %				100 %				100 %	

Strategies					
Technology		Pedagogy / Andragogy		Sustainable Development	
Simulations	✓	Clarification/Pauses	✓	Good Health & Well Being	✓
Presentation Tools					
Learning Management System		Group Discussion	✓	Quality Education	✓
		Hands-on Practice	✓		
		Debate	✓		
		Interactive Lecture	✓		
		Brainstorming	✓		

Designers					
Professional Experts		Higher Institution Experts		Internal Experts	
1	<name>, <industry name>, <email id>	1	<name>, <institution name>, <email id>	1	Mariya Joseph, Assistant Professor, School of Law,, SRMIST
2	<name>, <industry name>, <email id>	2	<name>, <institution name>, <email id>	2	<name>, SRMIST, <email id>

Code	PLCS24402T	Title	ARTIFICIAL INTELLIGENCE AND CYBER SECURITY	Category		Professional Core (Elective)	L	T	P	C
							3	1	2	5

Course Offering Department	School of Law	Pre-requisite Courses	Nil	Co-requisite Courses	Nil	Progressive Courses	Nil	Data Book / Codes/Standards	

Title & Content	Unit 1	Unit 2	Unit 3	Unit 4	Unit 5
Duration (hour)	18	18	18	18	18
SLO-1	Analyze the transformative impact of Artificial Intelligence (AI) on various sectors in the 21st century, including its implications for socio-economic systems and technological advancement.	Evaluate the evolution of laws surrounding Artificial Intelligence (AI), analyzing key legal frameworks and precedents to understand the development of AI law.	Analyze the provisions of the Personal Data Protection Bill 2018, identifying key principles and regulations for safeguarding personal data in the digital realm.	Analyze the key components necessary for determining the confidentiality of information within IoT systems..	Analyze and compare regulatory frameworks governing IoT in the European Union (EU) and the United States.
SLO-2	Evaluate the ethical and societal challenges posed by the widespread adoption of AI technologies, considering issues such as privacy, bias, and job displacement.	Critically appraise the components of a National Strategy for Artificial Intelligence, discerning its objectives, implementation mechanisms, and impact on socio-economic development.	Evaluate the recommendations outlined in the Sri Krishna Committee Report, synthesizing insights to understand the rationale behind proposed reforms in data protection and privacy laws.	Evaluate the ethical culture within IoT-related companies and its implications for information confidentiality.	Identify IoT characteristics with the potential to generate ethical challenges in various contexts.
SLO-3	Critically assess the applications of Artificial Intelligence in the medical field, including its potential to enhance diagnostics, treatment planning, and patient care.	Analyze the significance of Artificial Intelligence across various sectors, synthesizing case studies to illustrate its transformative potential in healthcare, finance, transportation, and other industries.	Assess the relationship between cyber security and artificial intelligence, discerning how AI technologies can both enhance and pose challenges to cybersecurity measures.	Define the Internet of Things (IoT) and trace its historical development to understand its evolution and impact.	Formulate ethical questions and principles tailored to the unique challenges of IoT technology.
SLO-4	**Tutorial:** Engage learners in analyzing case studies to understand AI's transformative potential and its implications for future development.	**Tutorial**: Present case studies showcasing diverse applications of Artificial Intelligence in various sectors such as healthcare, finance, and transportation.	**Tutorial :** Examine various threats to online privacy, including data breaches, surveillance practices, and algorithmic discrimination**.**	**Tutorial** : Explore various ethical principles and theories applicable to IoT contexts through	Tutorial: Research and compare regulatory frameworks in the EU and US and Provide guidance for navigating regulations effectively.

SLO-5	**Practice:** Conduct a comparative analysis of historical and contemporary examples to elucidate the transformative nature of AI in diverse industries, culminating in a group presentation highlighting key findings and implications for future development.	**Practice:** Organize a panel discussion on the legal personality of Artificial Intelligence, featuring experts from law, ethics, and technology fields, facilitating dialogue on the implications of granting legal rights to AI entities and potential regulatory frameworks.	Practice: Conduct a mock legislative debate on the Personal Data Protection Bill 2018, where participants role-play lawmakers and stakeholders to discuss and negotiate key provisions of the bill.	**Practice:** Participate in a workshop to assess and refine criteria for determining information confidentiality in IoT systems.	**Practice:** Analyze real-world case studies depicting ethical dilemmas in IoT-related companies regarding information confidentiality.
SLO-6	**Practice:** Group Discussion on the ethical implications of AI technologies in a simulated scenario, engaging in structured arguments and counterarguments to explore differing viewpoints on issues such as privacy invasion and algorithmic bias.	**Practice:** Engage in a policy analysis workshop to examine existing regulations and guidelines governing AI technologies, identifying gaps and proposing amendments to promote ethical and responsible AI development and deployment.	**Practice:** Organize a panel discussion featuring experts on data protection and privacy to analyze the Sri Krishna Committee Report, providing insights into the report's recommendations and potential implications for stakeholders.	**Practice:** Analyze case studies of IoT-related companies to understand and evaluate their ethical culture's influence on information confidentiality.	**Practice :** Participate in a simulation exercise to evaluate the effectiveness of regulatory frameworks in ensuring confidentiality, identifying gaps for improvement.
SLO-7	Formulate strategic approaches for integrating AI technologies in the use of drones, emphasizing their role in surveillance, logistics, and disaster response..	Assess the objectives and scope of a National Programme on Artificial Intelligence, examining its role in fostering innovation, research, and development within a country's AI ecosystem.	Critically examine the ethical and legal implications of internet of things (IoT) devices, analyzing issues related to data privacy, consent, and liability.	Explore a range of general ethical principles and theories applicable to IoT contexts, discerning their relevance and effectiveness..	Evaluate security measures, privacy concerns, and trust aspects within the IoT ecosystem.
SLO-8	Analyze the utilization of Artificial Intelligence in drone technology, elucidating its role in surveillance, logistics, and disaster management, discerning ethical and legal implications in deployment scenarios	Examine the legal implications of assigning personality to Artificial Intelligence entities, considering ethical, moral, and regulatory challenges in granting legal rights and responsibilities.	Evaluate the security, privacy, and trust aspects of IoT ecosystems, identifying vulnerabilities and proposing strategies for mitigating risks to user data and privacy.	Assess the role of governments in the IoT landscape, focusing on regulatory frameworks, ethical standards, and data confidentiality.	Examine the ethical culture of IoT-related companies and its influence on information confidentiality.
SLO-9	Evaluate the cybersecurity threats posed by AI-enabled technologies, examining potential vulnerabilities in critical infrastructure and proposing mitigation strategies to safeguard against cyber threats.	Critique the ethical considerations surrounding the development and deployment of AI technologies, exploring issues such as algorithmic bias, privacy infringement, and societal impact.	Analyze the concept of the right to privacy and data protection on the internet, exploring legal frameworks and international conventions aimed at safeguarding individuals' privacy rights.	Identify the historical milestones and technological advancements shaping the IoT's definition and evolution.	Assess India’s stake in the Internet of Things and its implications for information confidentiality and ethical practices.

SLO-10	**Tutorial:** Introduce ethical frameworks relevant to AI development and deployment.	**Tutorial** : Engage in group discussions to evaluate the effectiveness of current AI laws and propose recommendations for future legal and policy developments..	**Tutorial** : Facilitate hands-on exercises where learners analyze real-world case studies to understand how AI can both strengthen and pose challenges to cybersecurity.	**Tutorial:** Investigate regulations governing IoT confidentiality in the EU and the US.	**Tutorial:** Explore IoT ethical issues and principles and offer strategies for addressing ethical concerns in IoT design.
SLO-11	**Practice:** Collaboratively design a case study exploring the application of AI-driven diagnostic tools in healthcare settings, including considerations of data privacy, accuracy, and patient outcomes, and present findings in a multimedia format.	**Practice:** Conduct a mock legislative session to debate and draft proposed laws on Artificial Intelligence, engaging in role-playing exercises to simulate the legislative process and consensus-buildin..	**Practice:** Participate in a tabletop exercise simulating a cyber attack targeting IoT devices, where participants collaborate to identify vulnerabilities, respond to security breaches, and develop incident response plans.	**Practice:** Attend a series of seminars providing a comprehensive overview of the definition and historical development of the Internet of Things.	**Practice**: Engage in debates to discuss and explore diverse ethical dilemmas inherent in IoT technology, applying various ethical principles and theories
SLO-12	**Practice:** Participate in a tabletop exercise simulating a cyber attack leveraging AI, where participants work in teams to identify and respond to evolving threats, emphasizing communication, collaboration, and decision-making under pressure.	**Practice**: work in groups to identify strategic objectives, action plans, and performance metrics, for AI and presenting proposals to a panel of experts for feedback and evaluation.	**Practice:** Engage in a privacy impact assessment workshop, where participants assess the security, privacy, and trust aspects of a hypothetical IoT deployment, identifying risks and proposing mitigation strategies.	**Practice:** Engage in interactive exercises applying various ethical principles and theories to real-world scenarios in IoT contexts.	**Practice:**Participate in a workshop to gain practical experience in evaluating security measures in IoT systems.
SLO-13	Synthesize interdisciplinary knowledge to design and implement AI-driven solutions for healthcare challenges, incorporating principles of medical ethics, data privacy, and regulatory compliance into solution development.	Synthesize interdisciplinary perspectives to propose policy recommendations for the responsible governance of Artificial Intelligence, incorporating legal, ethical, and technological considerations.	Examine the evolving concept of privacy in the digital age, considering the impact of technological advancements and societal norms on individuals' expectations of privacy.	Formulate ethical questions and principles specific to IoT contexts to guide decision-making processes.	Apply ethical principles and theories to address confidentiality challenges within IoT systems, considering diverse ethical perspectives.
SLO-14	Propose innovative strategies for optimizing the use of AI in drone operations, considering factors such as environmental impact, safety regulations, and public perception in the design and implementation of drone-based systems.	Formulate strategic approaches for integrating Artificial Intelligence into public administration and governance structures, emphasizing transparency, accountability, and citizen engagement	Assess the various threats to privacy on the internet, including data breaches, surveillance practices, and online tracking, and propose measures to enhance privacy protections.	Evaluate security, privacy, and trust aspects within the IoT ecosystem to safeguard confidentiality.	Critically analyze governmental policies and regulations concerning IoT, discerning their impact on ethical standards and data confidentiality.

SLO-15	Formulate comprehensive risk management frameworks to address emerging cyber threats posed by AI technologies, integrating principles of cybersecurity, risk assessment, and policy development to enhance resilience in digital ecosystems.	Assess the ethical and legal ramifications of AI-driven decision-making processes, exploring issues of fairness, accountability, and transparency in algorithmic systems..	Synthesize interdisciplinary perspectives to propose ethical and legal frameworks for regulating privacy on the internet, incorporating principles of transparency, accountability, and user empowerment.	Synthesize insights from the ethical culture of IoT-related companies, historical developments of IoT, and governmental roles to inform ethical decision-making in IoT contexts	Explore the intersection of IoT technology and ethical principles through theoretical frameworks.
SLO-16	**Tutorial:** Present an overview of cybersecurity risks associated with AI-enabled systems, including data breaches and malicious use.	**Tutorial:** Examine case studies of countries that have successfully implemented national strategies for Artificial Intelligence.	**Tutorial:** Explore case studies illustrating privacy breaches, data misuse, and liability issues in IoT ecosystems.	**Tutorial:** Examine the company's policies and practices concerning information confidentiality.	**Tutorial:** Discuss strategies for building trust and implementing security measures and Provide recommendations for fostering a culture of security awareness.
SLO-17	**Practice:** Role-play a cybersecurity task force tasked with identifying and addressing potential vulnerabilities in AI systems used for critical infrastructure protection, culminating in a comprehensive risk assessment report and recommendations for mitigation strategies	**Practice:** Analyze case studies highlighting the impact of Artificial Intelligence in different sectors, synthesizing findings to identify common themes, challenges, and opportunities for future development.	**Practice:** Conduct a role-playing exercise where participants act as internet users navigating privacy challenges online, such as encountering targeted advertisements or data collection practices, and discuss strategies for protecting personal information.	Practice: Participate in a simulated scenario exploring the role of governments in regulating IoT, considering the implications for ethical standards and data confidentiality.	Practice: Engage in a stakeholder consultation session regarding India's involvement in the IoT industry and its impact on information confidentiality
SLO-18	**Practice**: Engage in a panel discussion with experts from various fields to examine the ethical, legal, and societal implications of AI technologies, fostering interdisciplinary dialogue and consensus-building on policy recommendations for responsible AI deployment.	**Practice:** Participate in an AI Ethics Workshop.	**Practice:** Organize a symposium on privacy in the digital age, featuring presentations from legal scholars, technologists, and activists to explore emerging threats to privacy on the internet and strategies for preserving digital freedoms**.**	Practice: Join a debate forum to discuss and debate governmental policies and regulations concerning IoT, exploring their ethical implications and potential impact on confidentiality.	Practice: Assess organizational practices and policies to identify strengths and areas for improvement in fostering a culture conducive to confidentiality
Assessment	Continuous Learning Assessment - 1				

Resources			
1	Akash Kamal Mishra, An Overview on Cyber Crime & Security, Createspace Publications, Second Edison:2018	6	PavanDuggal, Artificial Intelligence Law, Amazon Asia-Pacific Holdings Private Limited
2	Rear Admiral Dr. S. Kulshrestha (Retd.), Indian Navy,TheInterweaving of Cyber Security in Artificial Intelligence, IntraStra Global Publications, 2019	7	.SaiSundara Krishnan, Computational Intelligence, Cyber Security and Computational Models, Springer Publications, 2014,
3	Rear Admiral Dr. S. Kulshrestha (Retd.), Indian Navy, Artificial Intelligence & Cyber Defense, IntraStra Global Publications	8	PavanDuggal, Artificial Intelligence & Cyber Security Law, 2018
4	Xingming Sun, Artificial Intelligence and Security, Springer Publications, Switzerland, 2019	9	

Rationale (CLR)	The purpose of learning this course is to:	Depth				Attainment			Program Learning Outcomes (PLO)												
		1	2	3	4	1	2	3	1	2	3	4	5	6	7	8	9	10	11	12
CLR-1	Examine the transformative potential of Artificial Intelligence (AI) in the 21st century, explore its implications across diverse domains, tackle associated challenges, and evaluate its applications in medicine and drone usage, while also addressing methods to mitigate cyber threats resulting from AI integration.	Conceive	Design	Implement	Operate	Level of Thinking	Expected Proficiency (%)	Expected Attainment (%)	Disciplinary Knowledge	Critical Thinking	Problem Solving	Analytical Reasoning	Research-related Skills	Communication Skills	Cooperation/Team Work	Digital Literacy	Self-directed Learning	Moral and Ethical Reasoning	Leadership Qualities	Life Long Learning
CLR-2	Equip participants with the ability to examine a case study demonstrating practical applications of Artificial Intelligence (AI), understand the evolution of laws related to AI development, evaluate national strategies and programs for AI implementation in diverse sectors, and assess the concept of legal personality assigned to AI entities.																			
CLR-3	Assess the relationship between cybersecurity and artificial intelligence, scrutinize the ethics and laws regulating the Internet of Things, appraise security, privacy, and trust considerations, comprehend the right to privacy and data protection online, grasp the concept of privacy, and identify emerging threats to online privacy.																			
CLR-4	Evaluating factors influencing information confidentiality, such as the ethical culture of IoT companies, while also ensuring a comprehensive understanding of IoT's definition, historical context, ethical principles, governmental roles, regulations, characteristics, security, privacy, trust, ethical questions, and India's involvement in the field.																			
CLR-5	Explore IoT Governance & Ethics: Implementing Compliance, Principles, and Security Measures to Navigate Regulatory Landscapes and Ethical Challenges, Including Assessing India's Role in the Internet of Things																			
Outcomes (CLO)	At the end of this course, learners will be able to:																			
CLO-1	Evaluate the transformative potential of Artificial Intelligence (AI) in the 21st century, analyze its implications across various domains, address associated challenges, and assess its applications in the medical field, as well as in the utilization of drones while mitigating cyber threats posed by AI integration.	✓	✓		-	2	85	75	3	-	-	1	-	3	-	2	2	1	2	3
CLO-2	Analyze a case study illustrating the practical applications of Artificial Intelligence (AI), comprehend the evolution of laws concerning AI development, assess national strategies and programmes for AI implementation across various sectors, and evaluate the concept of legal personality attributed to AI entities.	✓	✓	✓	-	2	85	75	3	2	1	2	2	3	-	1	2	1	2	3
CLO-3	Evaluate the relationship between cybersecurity and artificial intelligence, examine the ethics and laws governing the Internet of Things, assess security, privacy, and trust considerations, understand the right to privacy and data protection online, grasp the concept of privacy, and identify emerging threats to online privacy.	✓	✓	✓	✓	3	85	75	3	1	3	1	3	3	-	1	1	2	1	3
CLO-4	Proficient in assessing factors influencing information confidentiality, including the ethical culture of IoT companies, alongside comprehending IoT's definition, historical context, ethical principles, governmental roles, regulations, characteristics, security, privacy, trust, ethical questions, and India's stake in the field.	✓	✓	✓	✓	3	85	75	3	3	2	3	3	3	-	2	3	3	3	3
CLO-5	Apply in navigating IoT regulatory frameworks, implementing compliance measures, applying ethical principles, ensuring robust security, and evaluating India's involvement in the Internet of Things.	✓	✓		✓	3	85	75	3	3	2	2	3	3	2	2	3	3	3	3

Assessment Method (Max. Marks: 100)																			
		Continuous Learning Assessment (CLA 40% Weightage)												Final Exam					
Level of Thinking		Model Exam (20%)				Assignment/ Seminar/Group discussion/ Presentation				Participation in seminar/ Conference/ Publication				Participation in class room/co-curricular & Para curricular activities					
		(20%)				(10%)				(5%)				(5%)				(60%)	
1	Remember	40%		-		40%		-		30%		-				-		40%	-
2	Understand																		
3	Apply	40%		-		40%		-		40%		-				-		40%	-
4	Analyze																		
5	Evaluate	20%		-		20%		-		30%		-				-		20%	-
6	Create																		
Total		100 %				100 %				100 %				100 %				100 %	

Strategies							
Technology			Pedagogy / Andragogy			Sustainable Development	
Simulations	✓		Clarification/Pauses	✓		Good Health & Well Being	✓
Presentation Tools	✓						
Learning Management System	✓		Group Discussion	✓		Quality Education	✓
			Hands-on Practice	✓			
			Debate	✓			
			Interactive Lecture	✓			
			Brainstorming	✓			

Designers					
Professional Experts		Higher Institution Experts		Internal Experts	
1	<name>, <industry name>, <email id>	1	<name>, <institution name>, <email id>	1	Dr. Ishita Chatterjee, Professor, School of Law, SRMIST
2	<name>, <industry name>, <email id>	2	<name>, <institution name>, <email id>	2	<name>, SRMIST, <email id>

DISSERTATION CORE FOUNDATION

Code	PLCS24403P	Title	DISSERTATION	Category	Core Practical (P)	L	T	P	C
						0	2	20	12

Course Nature: Practical					
Assessment Method (Max Marks:100)					
End-semester	Assessment Tools	Written- Submission	Presentation	Viva Voce	Total
	Marks	60	20	20	100
				Total Max Marks	100