


Name:			
Enrolment No:			
UPES End Semester Examination, May 2024			
Course: Information Technology Law		Semester: X	
Program: BA LLB/BBA LLB/B Com LLB (All Spez.)		Time: 03 hrs.	
Course Code: CLCC4006		Max. Marks: 100	
Instructions:			
SECTION A (5Qx2M=10Marks)			
S. No.		Marks	CO
Q1.	State any two documents or transactions to which the IT Act is not applicable.	2	CO1
Q2.	Describe two types of e-contracts commonly used in digital transactions.	2	CO1
Q3.	State the name of the Appellate Authority for adjudication of disputes under IT Act, 2000.	2	CO1
Q4.	State the definition of “cyber terrorism” as per the Information Technology Act,2000.	2	CO1
Q5.	State the SC judgment wherein the right to informational Privacy was declared as a Fundamental Right.	2	CO1
SECTION B (4Qx5M= 20 Marks)			
Q6.	Discuss the roles and functions assigned to controllers under the IT Act 2000.	5	CO2
Q7.	Explain the objectives and Significance of the Digital Data Protection Act, 2023.	5	CO2

Q8.	Differentiate between Cyber Contraventions and Cyber offences as per Information Technology Act 2000.	5	CO2
Q9.	Explain Cyber Voyeurism and discuss relevant provisions under the Information Technology Act, 2000.	5	CO2
SECTION-C (2Qx10M=20 Marks)			
Instruction: Kindly attempt any one of the choices given within each question.			
Q10.	<p>i) Explain the relevance of ‘Digital Signatures’ with diagrams. How does encryption and secret keys play a crucial role in ensuring the security and authenticity of digital signatures?</p> <p style="text-align: center;"><u>OR</u></p> <p>ii) Evaluate the enforceability of electronic contracts under Section 65 of the Indian Evidence Act with a focus on digital signatures and electronic records.</p>	10	CO3
Q11.	<p>i) Cyberspace is the virtual world where no territorial boundaries exist. It is the ‘transnational’ element of the borderless cyberspace, which leads to one of the most cryptic issue of jurisdiction. Discuss the various principles and tests to determine internet jurisdiction.</p> <p style="text-align: center;"><u>OR</u></p> <p>ii) Knowledge and intention are required to constitute the offence of tampering with computer source documents. Discuss the statement with a suitable example. Also state relevant case laws</p>	10	CO3
SECTION-D (2Qx25M=50 Marks)			
Instruction: Kindly attempt any one of the choices given within each question.			
Q12.	<p>12.1 A content creator on a widely used digital platform publishes a series of articles and videos that, while intended to be educational, contain explicit and graphic descriptions of sexual practices. The content sparks controversy, leading to complaints and a subsequent investigation under Section 67 of the Information Technology Act.</p>	25	CO4

	<p>A. Discuss the boundaries between freedom of expression and obscenity as defined under Section 67, particularly in digital and educational contexts. (10 Marks)</p> <p>B. Additionally, Assess the implications of this section for content creators, focusing on the legal criteria for determining what constitutes “obscenity.” (15 Marks)</p> <p style="text-align: center;"><u>OR</u></p> <p>12.2 In the world of digital transactions, the security of such transactions is also significant. The Information Technology Act has vested the Certifying Authority with this responsibility. Consider the following situation:</p> <p>A Certifying Authority “XYZ”, issued a digital signature certificate to Mr. A, a businessman. In due course of his business, his clients started raising objections to the authenticity of his digital signature. Reports of alleged suspension of licence of XYZ started emerging. Mr. A approaches you, a cyber lawyer to assist him about the dispute:</p> <p>A. Explain the legal action to be taken by XYZ if their licence is suspended as per the Information Technology Act, 2000. (15 Marks)</p> <p>B. Discuss the role of Controller in the above case as per the provisions of the Information Technology Act, 2000. (10 Marks)</p>		
<p>Q13.</p>	<p>Avika Birla, was the Managing Director of Ahazee, a company which provided an online platform and marketplace ahazee.com where sellers could list their goods and services, and buyers could choose whether they were interested in buying any services. An online payment facility was also provided by Ahazee, where Ahazee charged a commission of Rs. 3 per transaction (being charges involved in banking fees). It was found that an obscene advertisement for a pornographic video was listed on the website of Ahazee by Mr. Kavi Raj. The video was titled as “KV Girls having fun”; and the safety filters of Ahazee failed to detect this listing. The manual inspection revealed the possibility of pornographic material being listed, and the listing was removed from the website by Ahazee, within the period of a couple of days. However, within the short</p>	<p style="text-align: center;">25</p>	<p style="text-align: center;">CO4</p>

	<p>time period on which the listing was available for sale, a huge number of buyers purchased the videos. The prosecution filed a Charge sheet against the then Managing Director of Ahazee, accusing that he had committed offences under Section 292 of the Indian Penal Code and Section 67 of the Information Technology Act. Analyze the abovementioned facts and answer following questions:</p> <ol style="list-style-type: none">1) Whether an online marketplace website, Ahazee and its Ms. Avika could be held to have committed any offence under Section 67 of IT Act, 2000 because a pornographic video was listed on the website maintained by the company. (10 Marks)2) Explain the relevant provisions of IT Act and Judicial Precedents which may be used by Ms. Avika to seek exemption from any kind of imposition of liability under the Information Technology Act, 2000. (15 Marks)		
--	--	--	--