**UPES**

**End Semester Examination, December 2024**

**Course: Information Technology Law**

**Semester: IX**

**Program: B.Tech,LL.B** **Time: 03 hrs.**

**Course Code:** CLCC5019 **Max. Marks: 100**

**Instructions:**

| | | | |
|---|---|---|---|
| **SECTION A (5Qx2M=10Marks)** | | | |
| S. No. | Questions | **Marks** | **CO** |
| Q 1 | Define "cyber terrorism" under the IT Act, 2000 and mention the penalty for committing it. | **2** | **CO1** |
| Q 2 | Differentiate between "cyber contraventions" and "cyber offences" under the IT Act with suitable examples. | **2** | **CO1** |
| Q 3 | Identify the authority responsible for appointing the Controller of Certifying Authorities and summarize their primary functions. | **2** | **CO1** |
| Q 4 | Define “intermediary” under the IT Act and provide an example. | **2** | **CO1** |
| Q 5 | Discuss the legal validity of electronic records under the Indian Evidence Act, 1872 and apply this understanding to explain its significance in legal proceedings. | **2** | **CO1** |
| **SECTION B (4Qx5M= 20 Marks)** | | | |
| Q 6 | Analyze the responsibilities of the Controller of Certifying Authorities in ensuring compliance with the IT Act. | **5** | **CO2** |
| Q 7 | What are the eligibility criteria for a firm to apply for a license as a Certifying Authority under Rule 8 of the IT (Certifying Authorities) Rules? | **5** | **CO2** |
| Q 8 | Discuss the challenges in ensuring the authenticity and integrity of electronic evidence in legal cases. | **5** | **CO2** |
| Q 9 | Explain the role of the Data Protection Board established under the DPDP Act. How does it ensure compliance? | **5** | **CO2** |
| **SECTION-C (2Qx10M=20 Marks)** | | | |
| Q 10 | Evaluate the responsibilities of the Adjudicating Officer under the IT Act in resolving disputes related to cyber contraventions. Critically assess how the adjudication process ensures both fair compensation for victims | **10** | **CO3** |

| | | | |
|---|---|---|---|
| | and accountability for offenders, drawing on relevant provisions and practical implications. | | |
| Q 11 | Analyze the legal framework governing the liability of intermediaries under the IT Act when hosting user-generated content, particularly in cases involving content inciting communal violence. Apply the provisions to assess the validity of the platform's claim for "safe harbor" protection and propose practical reforms to balance accountability and innovation. | **10** | **CO4** |
| **SECTION-D<br>(2Qx25M=50 Marks)** | | | |
| Q 12 | ABC Secure Ltd., a newly incorporated company under the Companies Act, 1956, seeks a license to operate as a Certifying Authority under the IT Act, 2000. Although the company meets the paid-up capital requirement of 5 crores, it does not meet the standalone net worth requirement of 50 crores as specified in Rule 8. However, the majority shareholders of ABC Secure Ltd., holding at least 51% of the paid-up equity, are Indian citizens with a combined net worth exceeding 50 crores.<br>The Controller must assess the application, taking into account the eligibility requirements, the financial status of the company and its shareholders.<br>**In light of the above facts:**<br>**1.** Evaluate the authority of the Controller under Section 24 of the IT Act to grant the license to ABC Secure Ltd. given the company's reliance on the majority shareholders' net worth. **(5 marks)**<br>**2.** Critically analyze the categories who can apply for license along with the eligibility criteria for applying for a Certifying Authority license under Rule 8. **(15 marks)**<br>3. Based on your analysis, determine whether ABC Secure Ltd. should be granted the license, and provide a well-reasoned justification for your conclusion. **(5 marks)** | **25** | **CO5** |
| Q 13 | XYZ Healthcare Pvt. Ltd., a body corporate engaged in providing online healthcare services, stores sensitive personal data of its patients, including medical history, contact information, and financial details, on its digital platform. Due to a cyberattack, sensitive patient data is leaked, leading to financial fraud and identity theft for several users. Upon investigation, it is found that XYZ Healthcare Pvt. Ltd. had not implemented reasonable security practices and procedures under the IT Act. The affected patients file a claim for compensation under the Act.<br>Additionally, during the inquiry, the company fails to furnish the required information and documentation to the investigating authority within the specified time. The investigation also reveals that the company did not maintain proper records of its cybersecurity audits. | **25** | **CO5** |

| | | | |
|---|---|---|---|
| | **1.** Analyze whether XYZ Healthcare Pvt. Ltd. is liable to pay compensation under Section 43A of the IT Act for the data breach. Discuss the criteria for determining "reasonable security practices and procedures" and evaluate the company's negligence in this context. **(5 marks)**<br>2. Evaluate the implications of XYZ Healthcare Pvt. Ltd.'s failure to furnish documents and information within the specified time. Discuss the penalties applicable and their potential deterrent effect on non-compliant companies. In addition to the compensation claims and specific penalties under Sections 43A and 44, discuss whether XYZ Healthcare Pvt. Ltd. could also face a penalty under Section 45 for contravening other unspecified regulations related to data protection. **(15 marks)**<br>3. Suggest measures that XYZ Healthcare Pvt. Ltd. could adopt to comply with data protection regulations in the future. **(5 marks)** | | |