NATIONAL LAW UNIVERSITY, JODHPUR

(End Term Examination August-December 2025)

Semester: LL.M. (Law and Technology) (Semester I)

Subject: Data Protection and Cyber Security Law

Time: 03 Hours | Marks: 100

INSTRUCTIONS:

1. Attempt any **FOUR** questions out of the six.
2. All questions carry equal marks (25 Marks each).
3. Scholars are expected to refer to relevant statutory provisions and case laws.
4. Your answers should be analytical and well-structured. Focus on demonstrating a clear understanding of the interplay between technology, law.

Q.1). Discuss the philosophical and constitutional underpinnings of the right to privacy in India, tracing its evolution up to the Justice K.S. Puttaswamy (Retd.) v. Union of India judgment. How have the key principles from this judgment shaped the core obligations of "Data Fiduciaries" under the Digital Personal Data Protection (DPDP) Act, 2023? **(Marks 25)**

Q.2). Explain the foundational legal frameworks for cybersecurity in India under the Information Technology Act, 2000. Critically analyse the scope, objectives, and compliance requirements of the 2022 CERT-In Directions on Information Security Practices. **(Marks 25)**

Q.3). What are "Privacy-Enhancing Technologies (PETs)"? Discuss the principle of "Privacy by Design and Default" and its significance in modern IT governance. Further, explain the role and limitations of cyber-insurance policies in mitigating risks associated with data security.

(Marks 25)

Q.4). Define "Data Constitutionalism". Analyse the key legal and practical challenges that corporations and governments face concerning cross-border data flows and data localisation mandates. **(Marks 25)**

Q.5). "MediHealth Corp,"a private company managing the digital health records for several large hospitals in India, suffers a major ransomware attack. The attackers exfiltrate and encrypt sensitive personal data, including the medical histories of over one million patients. As the Legal Officer of MediHealth Corp, draft a comprehensive memorandum addressing the following:

a) Your immediate legal obligations for reporting this incident under the DPDP Act, 2023 and the MHA/CERT-In Directions. **(Marks 10)**

b) The potential liabilities of the company's directors for failing to ensure adequate board-level governance of cyber risk. **(Marks 5)**

c) A legal analysis of whether paying the ransom is advisable, considering the IT Act, 2000, and MHA directives. **(Marks 10)**

Q.6) An Indian FinTech startup, "FinSecure", is developing a new app that uses AI-driven "Open-Source Intelligence (OSINT)" to assess credit risk. This involves scanning a loan applicant's social media profiles and other publicly available data. The company plans to launch simultaneously in India and the European Union. Analyse the following:

a) The compatibility of this data processing model with the data minimisation and consent principles under the DPDP Act, 2023. **(Marks 10)**

b) The significant legal hurdles the company will face under the EU's General Data Protection Regulation, particularly concerning data transfers. **(Marks 5)**

c) The challenges in ensuring compliance with both regimes, referencing the principles laid out in the *Schrems* cases and the complexities of cross-border data transfers. **(Marks 10)**