LAMARK BIOTECH PRIVATE LIMITED

DATA PRIVACY AND PROTECTION POLICY

Policy Title:	**Data Privacy and Protection Policy**
Date & Version	**18th March, 2025; v1.0**
Applicable Laws:	**Digital Personal Data Protection Act, 2023 (DPDP Act)** **Information Technology Act, 2000**
Preamble & Objectives	1. Ensure strict compliance with all relevant data protection legislation. 2. Minimize the risk of unauthorized access and misuse of personal data through robust security measures. 3. Clearly define and document the purpose, nature, and lifecycle of all personal data handled by the company. 4. Protect individuals and the Company from potential harm and financial losses resulting from data breaches.
Scope & Applicability:	Applicable to all employees, trainees/interns, apprentices, contract workforce, vendors, customers, auditors, directors and visitors (collectively called 'personnel') of Lamark Biotech Private Limited and its subsidiaries (termed as Lamark Biotech or the Company in the policy).

Policy Details:

1. Background:

The Company understands the importance of the security of personal data*, its collection, use, and storage. Unauthorized possession or use of personal data could lead to misuse of the data, thereby causing harm to the individual and/or financial losses to the Company. Lamark Biotech strives to ensure legislative compliance concerning security of personal data, identifying the purpose of its usage, nature of the data being received, processed, managed, stored, and discarded. It is also important to ensure adequate safety and security measures to mitigate the risk of data loss or misuse through the implementation of this policy at the Company.

2. Principles and Guidelines:

The following principles guide our commitment to ensuring data privacy and protection:

a. Compliance with applicable regulations, or statutory requirements, on protection of personal data as per the applicable laws of India.

b. Personal data will be collected in a fair, transparent and lawful manner, and personal identifiable information collected from third parties will be reliable and legally obtained.

c. Adequate care shall be taken to ensure that personal data collected is sufficiently protected against any breach or loss.

d. Employees/stakeholders are given adequate training on personal data protection and their responsibility while handling such data.

e. Adequate care is taken by third parties who collect/manage/process personal data on behalf of the

Company to ensure data safety.

f. Personal data, which the Company collects, is used expressly for legitimate activities and only for the purpose consented by the individual.

***Personal Data:**

Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

The following is categorized as personal data, which is covered under this document, including without limitation:

a. Racial or ethnic origin,

b. Political or ideological opinion or activities,

c. Religious or philosophical beliefs,

d. Trade union-related views or activities,

e. Physical or mental health or medical records/history,

f. Administrative or criminal proceedings and sanctions,

g. Biometric data (e.g., physical, physiological, or behavioral characteristics, including, but not limited to, facial images, genetic information, fingerprints, handprints, footprints, iris recognition, handwriting, typing dynamics, and speech recognition),

h. Financial information/details (such as bank account number, credit card details, etc.),

i. Any other PII (Personal Identifiable Information - e.g., name, telephone number, date of birth, email IDs, unique government identification number, etc. as may be prescribed by the applicable laws),

3. Compliances with the policy

Guided by the principles mentioned in this policy, the Company will endeavor to ensure the following:

3.1 Collection of Personal Data directly or indirectly from an individual:

a. Ensure that data subjects are informed (to the extent applicable, on a case-to-case basis), in writing or by electronic means, and their explicit consent is obtained before collection/ processing of personal data.

3.2 Processing and storage of Personal Data:

a. Data collected for specified, explicit and legitimate purposes are not processed in a manner that is incompatible with those purposes.

b. Embed physical and information technology measures across the organization for preventing data loss, unauthorized access, misuse, alteration, damage or destruction that can occur during the processing and storage of personal data.

c. Adequate training is given to the personnel on the importance of data privacy, integrity, and confidentiality.

3.3 Data Retention and Data Disposal:

a. Undertake reasonable steps to ensure that no personal data is retained any longer than is necessary or as applicable by any legal requirement.

b. Take appropriate measures to ensure that records/data which are being disposed of after the retention period go through adequate checks, which restrict data leakage.

c. The policy related to data retention and data disposal is applicable on all employees, personnel, contractors, consultants, and third parties engaged by the Company and includes data, without limitation, electronic and physical records, customer and employee data, research data, financial records, and intellectual property, whether or not in the form of confidential data, personal data, operational data, or public data.

d. Data disposal shall be carried out in the following manner:

- Electronic Data: Must be permanently deleted using secure wiping software or degaussing, purging, media destruction, disk degaussing, multiple data overwrite, etc., such that it leaves no possibility for the reconstruction of the documents and information contained therein. Tapes shall be destroyed by magnetic tape shredders before disposal.
- Physical Records: Must be shredded or incinerated or similar methods to prevent unauthorized access, such that it leaves no possibility for reconstruction of the documents and information contained therein. Non-confidential paper documents can be recycled.
- Backup Data: Backups containing obsolete data must be securely erased.
- End-of-Life Devices: Hard drives and other storage media must be destroyed before disposal.

e. If the documents are maintained with a third-party service provider, those shall be destroyed only upon approval from the CEO of the Company and a confirmation shall be obtained from the service-provider indicating that the documents have been destroyed in line with the requirements of Company policy. These documents shall be destroyed only in the presence of a representative from the Company.

f. If personnel have reasons to believe, or the Company informs the personnel concerned, that Company documents are relevant to litigation, or potential litigation (i.e., a dispute that could result in litigation), then the personnel must preserve those until legal or respective department determines that the documents are no longer needed. This exception supersedes any previously or subsequently established retention schedule for those documents.

3.4 Data Processing by a third party on behalf of the Company:

a. The Company will establish and maintain a valid contract with any third party that processes personal data. The contract must include robust data protection clauses and mandate the use of secure data transfer channels.

b. The Company will strive to engage third parties, that may need to access such personal data, that demonstrate sufficient guarantees of existing compliance or commit to implementing appropriate technical and organizational measures to ensure the protection of data subjects' rights.

4. Governance:

a. The Management of the Company will undertake periodic review and update this policy. The personnel of the Company will review compliance with this policy and its effectiveness.

b. Changes to this policy will be approved by the Management of the Company, in consultation with its IT and Legal personnel/team.

c. The Company will ensure periodic training on this policy to all employees, trainees, contract workforce, consultants, and apprentices.

d. Any violation of this policy may have significant consequences and will be dealt with according to the Company's code of conduct and other relevant policies, such as disciplinary action, termination, and other legal actions.

5. Implementation:

Respective personnel (acting on behalf of Lamark Biotech) are responsible for adhering to the principles set out in this policy. They will familiarize themselves with this policy and participate in all training sessions periodically conducted by the Company. Any concerns or non-compliance with this document can be informed to the Rajat Bhatia (relevant personnel/team).