Marksans Pharma Ltd.

Regd. Office
11th Floor, Grandeur, Veera Desai Extension Road, Oshiwara, Andheri (W), Mumbai – 400053

MARKSANS DATA PRIVACY AND SECURITY POLICY

Table of Contents

1. Introduction

Marksans Pharma Limited ("Marksans") is committed to data privacy and data security. We strive to apply and integrate reasonable and appropriate information security controls within the organization's working environment, to ensure information protection from cyber threats to confidentiality, integrity and availability, thereby enhancing confidence/assurance to all the stakeholders.

2. Scope

This Policy outlines the governance structure for data privacy and protection matters, guidelines for collecting and using personal information, mechanism for monitoring compliance and grievance redressal.

This Marksans Data Privacy and Security Policy ("Policy") is applicable to Marksans's manufacturing plants, R & D centers, offices, subsidiaries, contractors, consultants, interns, trainees, service providers, customers, and business partners who may have access to or receive Personal Data from Marksans, or who provide Personal Data to Marksans.

This Policy applies regardless of where the processing of Personal Data happens, or whether the Processing is wholly or partly automated, or manually as part of a structured filing system. Wherever the context requires in the Policy, Personal Data shall be construed to also include Sensitive Personal Data.

3. Principles and Guidelines

Marksans shall abide by the following principles when managing Personal Data:

- Processing of Personal Data shall be done lawfully, fairly and transparently, regardless of the source of Personal Data.
- Personal Data shall only be collected and processed for specific, explicit and legitimate purposes.
- Personal Data collected shall be adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected. No more than the minimum amount of data shall be retained for processing.
- Personal Data shall be accurate and up to date. Upon receipt of request from the Data Subject, inaccurate data shall be rectified or erased.
- Personal Data which is no longer required shall be removed or erased.
- Adequate security controls shall be implemented for protection against unauthorized processing, loss, damage, and destruction.

Guided by these principles, Marksans shall:

- uphold rights of Data Subjects and address their concerns through the data protection office;
- inculcate a culture of data protection and privacy to sustain awareness and adhere to global data protection laws;
- embed privacy-by-design in organizational processes;

- retain Personal Data only for as long as necessary to fulfil the purposes of collection or as required by law;
- ensure that access to Personal Data is given only to authorized persons on need-to-know basis;
- ensure adequate security controls are in place when transferring Personal Data across jurisdictions or to any third party through means of contracts, data transfer agreements, or to the extent allowed by law;
- record and report all data breaches to the data protection office, the relevant regulatory authority, and the affected Data Subjects within prescribed timelines;
- confirm adherence to this policy through regular audits and monitoring systems;
- take timely remedial measures against all breaches to this Policy;
- encourage adherence to this Policy by imbibing this as an inherent part of work culture.

4. System & Data Security

- This Policy applies to all authorized users to access the company's IT facilities and ensure the security of all IT installation across the company. In order to maintain the security of IT infrastructure, following should be kept in mind while installing the IT infrastructure:

Server Room:

- The vulnerability of business-critical information systems and the data they contain within the Server Room make the site a high value asset which requires a high degree of protection. A range of security measures are therefore in place to protect information and physical assets, along with the reputation of the company.
  a. Proper temperature to be maintained.
  b. Avoidance of water pipes and other moisture creating stuff.
  c. Separate/additional power backup should be available.
  d. Limited and strictly authorized access to server room.
  e. Biometric access control system is installed for entry for authorized users. Individuals with thumb access to the server room are responsible for ensuring the area remains secure upon entering or exiting.

System Security

- All devices owned by the organization or allowed on the organization network must be identified by their IP address to the IT department before being connected. (Possibly require static IP address).
- Each device user must be identified by name and information must be given to the IT department.
- All computers must be loaded with anti-virus program approved by IT department with the latest possible virus database updates.
- The operating system and application patches must be loaded on all computers/laptops etc. as and when they are circulated by the principal supplier/company.
- Any data stored on computers other than the server shall be the responsibility of the concerned user in terms of safety and backup.
- It shall be ensured that unauthorized persons cannot gain access to the computer without a proper user identification and password.
- User access shall be locked/unregistered by the administrator from the computer/network/system in-case of employee is on longer leave/vacation and/or terminated from the service.

- If required, the user access shall be provided based upon the approval from respective HOD
- All employees and personnel that have access to organizations computer systems must adhere to the approved application (software) policy in order to protect the security of the network, protect data integrity, and protect computer systems. Software deemed safe and necessary shall only be installed in consultation of IT department having proper user licenses. All employees must follow these instructions as mentioned for software policy.
- No software or application shall be loaded without proper licenses.
- Only licensed software's should be installed in the company's network devices
- If the employee causes a security problem on the network by installing and running an unapproved program, they risk disciplinary action.
- The purchase, installation, configuration, support and record keeping of all licensed software and software application used within Marksans Pharma Ltd. are the responsibility of the IT department.

5. Cyber Security

- This Policy applies to all authorized users to access the company's IT facilities and ensure the security of all IT installation across the company. In order to maintain the security of IT infrastructure, following should be kept in mind while installing the IT infrastructure:

Server Room:

- The vulnerability of business-critical information systems and the data they contain within the Server Room make the site a high value asset which requires a high degree of protection. A range of security measures are therefore in place to protect information and physical assets, along with the reputation of the company.
  a. Proper temperature to be maintained.
  b. Avoidance of water pipes and other moisture creating stuff.
  c. Separate/additional power backup should be available.
  d. Limited and strictly authorized access to server room.
  e. Biometric access control system is installed for entry for authorized users. Individuals with thumb access to the server room are responsible for ensuring the area remains secure upon entering or exiting.

User Access Management:

a. No unauthorized access to computers and data is allowed.
b. All users must be registered by creating their account, password and privileges.
c. Marksans network access shall not be allowed to the personal devices like Laptop, Computer, Tablet etc.

User Account and Password:

a. All users must have access account created by System administrator to access the network.
b. Initial password shall be created by the system administrator.
c. User account password shall be generated by respective user.
d. Computer must be password protected.
e. Password policy (password complexity) will be set as per internal procedure.
f. Users are responsible for the security of their password which they should not divulge, even to colleagues.
g. Password shall not be saved to respective application, browser etc.

6. Governance

Robust data protection controls and risk response mechanisms are followed to cater to protection of personal data within Marksans ecosystem. The Audit Committee of Marksans is the monitoring agency of this Policy and will also review complaints/breaches related to data privacy and security, and actions taken thereon, as a part of its governance and oversight responsibilities.

7. Training and Awareness

Employees shall be adequately made aware of their dos and don'ts through awareness training. Every manager shall make sure that their respective teams have received all necessary training and are fully aware of their responsibilities in terms of information security.

8. Grievance Redressal

Any query with respect to data privacy and grievances with respect thereto can be addressed to the Company Secretary & Compliance Officer through e-mail at companysecretary@marksanspharma.com. Upon receipt of the communication, Marksans' IT Department will examine and address the query/grievance raised as per internal policies and guidelines.

9. Change in Policy

Audit Committee of Marksans reserves the right to review this Policy from time to time and amend this Policy to reflect technological advancements, legal and regulatory changes and good business practices.

This Policy is approved by the Audit Committee of Marksans and is effective from 13th February 2023.