SMS LIFESCIENCES INDIA LIMITED

[Policy on Cyber Security and Data Privacy]

INTRODUCTION

Policy on Cyber Security and Data Privacy **("Policy")** of SMS Lifesciences India Limited **("Company")** is formulated pursuant to Regulation 27(2)(ba) of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 and notice issued by Stock Exchange dated 29th September, 2023. Further, the risk of data theft, scams, and security breaches can have a detrimental impact on a Company's systems, technology infrastructure and reputation. Consequently, the Company has created this policy to help outline the security measures put in place to ensure information remains secure and protected.

This Policy shall be available at the website of the Company at www.smslife.in/policies.php

OBJECTIVE AND PURPOSE

The purpose of this Policy is to

- protect Company's data and infrastructure;
- outline the protocols and guidelines that govern cyber security measures;
- define the rules for company and personal use; and
- list the Company's disciplinary process for policy violations.

SCOPE

This policy applies to all employees, contractors, volunteers, suppliers, interns, and/or any individuals with access to the electronic systems, information, software, and/or hardware of the Company and its subsidiaries.

CONFIDENTIAL DATA

Company defines "confidential data" as:

- Unpublished and classified financial information.
- Customer, supplier, and shareholder information.
- business processes, and/or new technologies.
- Employees' passwords, assignments, and personal information.
- Company contracts and legal records.

DEVICE SECURITY:

Company Use:

In order to ensure the security of all Company-issued devices and information,

All Employees are required to:

- Keep all company-issued devices, including tablets, computers, and mobile devices, password-protected (minimum of 8 characters).
- Secure all relevant devices before leaving their desk.
- Obtain authorization from the HR Manager and/or respective Dept. head before removing devices from Company premises.
- Refrain from sharing private passwords with coworkers, personal acquaintances, senior personnel, and/or shareholders.
- Regularly update devices with the latest security software.

Personal Use:

Company recognizes that employees may be required to use personal devices to access Company systems. In these cases, employees must report this information to management for recordkeeping purposes. To ensure Company systems are protected.

All Employees are required to:

- Keep all devices password-protected (minimum of 8 characters).
- Ensure all personal devices used to access company-related systems Share password protected.
- Install antivirus software.
- Regularly upgrade antivirus software.
- Lock all devices if left unattended.
- Ensure all devices are protected at all times.
- Always use secure and private networks.

The Board of Directors shall ensure that a Structured Digital Database (SDD) is maintained containing the names of such persons or entities, as the case may be, with whom UPSI is shared under Regulation 3 of Insider Trading regulations along with the Permanent Account Number (PAN) or any other identifier authorized by law, where PAN is not available. SDD shall be maintained internally with adequate internal controls and checks, such as time stamping, audit trails, etc. to ensure non-tampering of the database.

EMAIL SECURITY:

Protecting email systems is a high priority as emails can lead to data theft, scams, and carry malicious software like worms and bugs.

Therefore, Company requires all employees to:

- Verify the legitimacy of each email, including the email address and sender name.
- Avoid opening suspicious emails, attachments and clicking on links.
- Avoid clickbait titles and links.
- Contact the IT department regarding any suspicious emails.

TRANSFERRING DATA

Company recognizes the security risks of transferring confidential data internally and/or externally. To minimize the chances of data theft, we instruct all employees to:

- Refrain from transferring classified information to employees and outside parties.
- Only transfer confidential data over authorised Company' networks.
- Obtain the necessary authorization from senior management.
- Verify the recipient of the information and ensure they have the appropriate security measures.
- Immediately alert the IT department of any breaches, malicious software, and/or scams.

(Company shall compile all the details of Cyber Security incidents or breaches or loss of data or documents and submit the same to Stock Exchanges in the Corporate Governance Report on a quarterly basis.)

DISCIPLINARY ACTION:

Violation of this policy can lead to disciplinary action, up to and including termination.

Company' disciplinary protocols are based on the severity of the violation. Unintentional violations only warrant a verbal warning, frequent violations of the same nature can lead to a written warning, and intentional violations can lead to suspension and/or termination, depending on the case circumstances.

****

This policy was reviewed and approved in the Board meeting held on 10th February, 2024