GLOBAL BUSINESS INFORMATION PROTECTION POLICY

1. Overview

Confidential information is one of the most valuable assets of Cohizon Life Sciences Limited (erstwhile known as "Sajjan India Limited") (the "Company"), offering a significant competitive edge in the industry. Proper protection of such information is essential to maintaining the Company's business integrity and market position. Any lapse in safeguarding confidential data could lead to reputational harm and operational setbacks.

This document establishes the guidelines and responsibilities for handling confidential information at the Company. All employees, contractors, and third parties who interact with the Company's sensitive information must adhere to the directives outlined in this policy.

"The Company" refers to Cohizon Life Sciences Limited and its global subsidiaries, and this policy is applicable to all employees, globally.

2. Policy Objective and Scope

The purpose of this policy is to set clear standards for managing and safeguarding confidential and proprietary information at the Company. These standards apply not only to the Company's internal information but also to third-party confidential data shared with the Company in the course of business.

the Company operates in multiple legal jurisdictions and complies with all applicable data protection laws, including trade secret regulations. This policy provides an additional framework for structured information management, ensuring both legal compliance and best-in-class operational practices. The guidelines presented help ensure that access to sensitive data is granted only to those employees with a legitimate need, while limiting risks associated with unauthorized disclosures.

For effective implementation, the Company's information must be categorized into four classifications: Strictly Confidential, Confidential, Internal, and Public.

- **Strictly Confidential** refers to data that, if disclosed, could cause significant harm to the Company's business, such as strategic plans, proprietary processes, or sensitive financial details.
- **Confidential** applies to data that is critical to day-to-day operations but with broader access compared to Strictly Confidential information.
- **Internal** covers information shared among employees but not intended for external parties.
- **Public** refers to data that is openly available and accessible to all.

3. **Employee Roles and Responsibilities**

a. **Non-Disclosure and Confidentiality Agreements:**
All employees are expected to sign confidentiality agreements that bind them to protect the Company's confidential information and restrict its use solely to fulfilling their job roles. This responsibility extends beyond the signing of agreements, meaning employees are bound to these obligations whether or not formal documentation is in place. Newly hired employees should review and sign confidentiality agreements during onboarding.

b. **Handling of Third-Party Information:**
The Company respects the confidential information and intellectual property of its business partners and third parties. Employees must not use or disclose third-party data without explicit permission. This includes avoiding the use of confidential data from former employers or other organizations without proper authorization. Any accidental access to third-party information should be reported immediately to a supervisor or legal counsel.

c. **Invention and Intellectual Property Rights:**
Any intellectual property, inventions, or developments created by employees in the course of their work at the Company are the property of the Company. Employees are required to assign all rights to such creations to the Company as detailed in the Company Intellectual Property Policy.

d. **Exit Protocols:**
When employees leave the organization, HR, IT, and their supervisor will collect company assets such as devices, key cards, and documents. Access to company systems will be terminated, and the Company will ensure that all confidential data is removed from personal devices. During exit interviews, departing employees will be reminded of their continuing obligations regarding confidential information.

4. **3. Third-Party Data Disclosure Guidelines**

a. **Confidentiality Agreements with External Parties**:
Confidential information should only be shared with external entities when it is essential to achieve business objectives. In such cases, proper confidentiality agreements must be executed, ensuring that third-party recipients are legally bound to protect the Company's information. Such agreements must cover non-disclosure and limited use of shared information, with provisions in place for continuous protection as long as the information remains confidential.

b. **Public Communications and Disclosures**:
The Company believes in transparent communication with its stakeholders. However, when engaging with the public or external entities, only authorized personnel should represent the Company, ensuring that no sensitive data is inadvertently disclosed.

Reviews of speeches, presentations, and publications should be conducted by relevant departments prior to any public engagement.

c. **Regulatory Submissions**:
The Company is committed to complying with all legal requirements regarding information disclosure to regulatory bodies. While submitting mandatory filings or data to authorities, the Company ensures that confidential treatment is requested for sensitive information where possible. The compliance team will assess each case and exercise discretion in handling submissions to maintain confidentiality without impeding legal obligations.

5. Information Classification and Access Control

Proper classification of information is crucial to protect sensitive data while allowing appropriate access for business operations. The team responsible for generating data or documents must categorize the information into one of the following:

- **Strictly Confidential:** Critical business information with the highest level of protection.
- **Confidential:** Information restricted to senior management and key personnel.
- **Internal:** Information shared within the company but not for external parties.
- **Public:** Information freely accessible by the public.

This classification system should be communicated to all employees, with periodic training on proper handling, labeling, and access restrictions for each category.

6. Implementation, Monitoring, and Response Protocols

a. **Adoption of Specific Procedures:**
Regional offices and business functions are encouraged to adopt localized security measures consistent with this policy. For physical security, offices may implement restricted access zones, visitor logs, and secure filing systems. Employees are required to lock away documents containing sensitive information and ensure that physical assets are stored securely.

b. **Physical and Digital Security Measures**:
At the Company, various efforts in the form of physical security measures shall be taken to always protect its Highly Confidential and other valuable information. These measures are in addition to the ones mentioned above in this Policy, i.e., executing confidentiality agreements, identifying and classifying information, conducting exit interviews, etc.

Key Company's offices shall have appropriate physical barriers installed, as needed, with limited and strict visitor access to ensure that no unauthorized personnel enter the premises. Measures appropriate to the facility in question, such as maintaining

logbooks, conducting security checks, escorting visitors, and limiting their access inside the premises, issuing company badges, and retention and disposal of documents in a compliant manner, shall be adopted and followed.

All physical embodiments of Highly Confidential information, whether a prototype, working model or actual embodiment in use, shall be maintained in a restricted area that is under lock and key and out of public view. Employees or contractors shall put working materials or files containing Highly Confidential Information in a locked desk or filing cabinet when not in use.

Digital or electronic safety of Highly Confidential Information is also paramount. Relevant teams and stakeholders should liaise with local IT teams to set up safety processes/systems, as required, for adequate protection.

c. Information Sweep or Audit:

To ensure successful implementation of this policy, relevant teams who own Highly Confidential information should routinely conduct internal audits or "sweeps" to determine whether the measures in place are effective and whether additional measures need to be put in place. While conducting such sweeps, teams should include in their scope, major company devices, relevant documents, electronic servers, as well as physical locations including offices, laboratories, manufacturing facilities, vendor/customer sites etc. Relevant audit teams must be formed to carry such internal audits and sweeps.

Such an exercise will assist in taking stock of all the Highly Confidential information available to the relevant team and providing both general and targeted feedback on what can be done to both strengthen the protection of current information and ensure ongoing implementation of protections measures in the future.

The key questions that a team should ask themselves for conducting an effective Highly Confidential information sweep should be: What are the measures in place to protect the information? Where is the information located? Who has access to it? What can be done to further safeguard such information? Should further awareness sessions be carried out for employees to strengthen their understanding of protection measures? Is it better document labeling required to protect information? Are all policy statements in this policy being followed?

Based on routine information audits conducted by relevant teams and stakeholders, the procedures to be followed by the teams may be modified, or the policy itself may be updated and, if required, formal programs may be instituted for specific needs of such teams.

Please refer, for example, to the Information Security Management System, established by the IT team for this purpose.

d. Detection and Response Plan

Relevant teams should put in place appropriate mechanisms, including setting up focused committees or working groups, to timely detect leakage of the Company's private business information. It is the responsibility of all employees and third parties to use the Company's information to note and report any such incident to supervisors or other appointed contact persons in the relevant teams. Further, relevant teams should coordinate with their local Legal, HR or the IT department, as appropriate, for further assistance with investigation and response, depending on the kind of breach.

This policy has been approved and implemented by the Management with immediate effect.

Rajesh Kumar Srivastava, MD & CEO
Effective Date:- September 16, 2024
Revision No: 01