

# PRAGMETIS PHARMACTIVES LLP.

Plot. No. 1115, Kerala GIDC, Tal. Bavla, Dist.  
Ahmedabad-382220, Gujarat, India.



## **BUSINESS ETHICS POLICY**

**April 01, 2025**

# **BUSINESS ETHICS POLICY**

## **Content of Table**

| <b>Sr. No.</b> | <b>Topic Name</b>   | <b>Page No.</b> |
|----------------|---|-----------------|
| <b>1.0</b>     | <b>Applicability</b>  | 04              |
| <b>2.0</b>     | <b>Scope</b>  | 04              |
| <b>3.0</b>     | <b>Responsibility</b>   | 04              |
| <b>4.0</b>     | <b>Policy</b>   | 04              |
| 4.1            | Anti-Bribery and Corruption                                   | 05              |
| 4.2            | Anti-Competitive  | 06              |
| 4.3            | Information Security Management                               | 08              |
| 4.3.1          | Company approach to Data Protection                           | 09              |
| 4.3.2          | Data Breach and Reporting                                     | 09              |
| 4.3.3          | Cyber Essentials  | 10              |
| 4.3.4          | Farewell  | 10              |
| 4.3.5          | Devices   | 10              |
| 4.3.6          | Access Control  | 10              |
| 4.3.7          | Updates   | 11              |
| 4.3.8          | Virus Protection  | 11              |
| 4.3.9          | Physical LAN Security, Hubs/Switches LAN (Local area network) | 11              |
| 4.3.10         | Work Station  | 11              |
| 4.3.11         | Inventory Management  | 12              |
| 4.3.12         | Internet Security   | 12              |
| 4.3.13         | Email Security  | 12              |
| 4.3.14         | Data Storage  | 13              |
| 4.3.15         | Data Retention Schedule                                       | 14              |
| 4.3.16         | Encryption and Anonymization Data                             | 14              |
| 4.3.17         | Prohibited Activities   | 15              |

**Prepared By:**



**Ms. Kavita Jain**  
**(DGM-HR)**  
**Date: 01/04/2025**  
Rev. No. 00

**Approved By:**



**Mr. Anurag Hitkari**  
**(Managing Partner)**  
**Date: 01/04/2025**  
Page 2 of 26

## **BUSINESS ETHICS POLICY**

|     |        |  |    |
|-----|--------|--|----|
|     | 4.3.18 | Reporting Security Incidents                 | 16 |
| 4.4 |        | Anti-money laundering                        | 16 |
| 4.5 |        | Conflict of Interest                         | 18 |
| 4.6 |        | Fraud Prevention                             | 19 |
|     | 4.6.1  | Action Constituting Fraud                    | 19 |
| 4.7 |        | Whistle Blower                               | 20 |
|     | 4.7.1  | Preamble                                     | 20 |
|     | 4.7.2  | Purpose                                      | 21 |
|     | 4.7.3  | Applicability                                | 21 |
|     | 4.7.4  | Important Feature of the policy              | 21 |
|     | 4.7.5  | Complainant                                  | 22 |
|     | 4.7.6  | Protection                                   | 22 |
|     | 4.7.7  | Authority                                    | 23 |
|     | 4.7.8  | Reporting                                    | 23 |
|     | 4.7.9  | Investigation                                | 23 |
|     | 4.7.10 | Communication                                | 24 |
|     | 4.7.11 | Flexibility                                  | 24 |
|     | 4.7.12 | Complainant & Responsibility                 | 24 |
|     | 4.7.13 | Role of Investigation Authority              | 24 |
|     | 4.7.14 | Action Taken Report                          | 25 |
| 4.8 |        | Approval Procedure for Sensitive Transaction | 26 |

### **1.0 APPLICABLE**

**Prepared By:**



**Ms. Kavita Jain  
(DGM-HR)  
Date: 01/04/2025  
Rev. No. 00**

**Approved By:**



**Mr. Anurag Hitkari  
(Managing Partner)  
Date: 01/04/2025  
Page 3 of 26**

## **BUSINESS ETHICS POLICY**

This Policy shall be applicable from 01<sup>st</sup> of April 2025.

### **2.0 SCOPE**

Using the Business Ethics Policy, Pragmetis Pharmactives LLP. strives to create a productive work environment. Pragmetis Pharmactives LLP. also focuses on and expects all its employees, contractual staff, vendors, suppliers, business associates and other stakeholders to abide by this value system and policy as laid down hereunder.

### **3.0 RESPONSIBILITY**

Top Management

### **4.0 POLICY**

A written statement that clearly defines our company's approach to managing labour issues. This should include commitments to:

- Implementing the ETI Base Code.
- Adhering to all customer requirements, including customer-specific codes of conduct.
- Regulatory compliance.
- Continual improvement in social responsibility performance.

The scope of the policy should include all of the labour standards of the ETI Base Code, including:

- Employment is freely chosen.

**Prepared By:**



**Ms. Kavita Jain**  
**(DGM-HR)**  
**Date: 01/04/2025**  
Rev. No. 00

**Approved By:**



**Mr. Anurag Hitkari**  
**(Managing Partner)**  
**Date: 01/04/2025**  
Page 4 of 26

## **BUSINESS ETHICS POLICY**

- No harsh or inhumane treatment is allowed.
- Working conditions are safe and hygienic.
- Child labour shall not be used.
- Working hours are not excessive.
- No discrimination is practiced.
- Regular employment is provided.

### **4.1 Anti-Bribery and Corruption:**

PRAGMETIS PHARMACTIVES LLP. Anti-Bribery and Corruption Policy requires compliance with the highest ethical standards and all anti-corruption laws applicable in the countries in which PRAGMETIS PHARMACTIVES LLP. (whether through a third party or otherwise) conducts business. It requires all PRAGMETIS PHARMACTIVES LLP. employees and any third party acting for or on behalf of PRAGMETIS PHARMACTIVES LLP. to ensure that all dealings with third parties, both in the private and government sectors, are carried out in compliance with all relevant laws and regulations and with the standards of integrity required for all PRAGMETIS PHARMACTIVES LLP. business. PRAGMETIS PHARMACTIVES LLP. values integrity and **transparency and has zero tolerance for corrupt** activities of any kind, whether committed by PRAGMETIS PHARMACTIVES LLP. employees, officers, or third-parties acting for or on behalf of the PRAGMETIS PHARMACTIVES LLP..

**Corrupt Payments** - PRAGMETIS PHARMACTIVES LLP. employees and any third party acting for or on behalf of PRAGMETIS PHARMACTIVES LLP., shall not, directly or indirectly, promise, authorize, ratify or offer to make or make any

**Prepared By:**



**Ms. Kavita Jain**  
**(DGM-HR)**  
**Date: 01/04/2025**  
Rev. No. 00

**Approved By:**



**Mr. Anurag Hitkari**  
**(Managing Partner)**  
**Date: 01/04/2025**  
Page 5 of 26

## **BUSINESS ETHICS POLICY**

“payments” of “anything of value” to any individual including a “government Official” for the improper purpose of influencing or inducing or as a reward for any act, omission or decision to secure an improper advantage or to improperly assist the company in obtaining or retaining business.

**Government Officials** — Although PRAGMETIS PHARMACTIVES LLP.’s policy prohibits payments by PRAGMETIS PHARMACTIVES LLP. or third parties acting for or on its behalf to any individual, private or public, as a “quid pro quo” for business, due to the existence of specific anticorruption laws in the countries where we operate, this policy is particularly applicable to “payments” of “anything of value”, or at the request of, “government officials”.

**Facilitating Payments** — for the avoidance of doubt, facilitating payments (otherwise known as “greasing payments” and defined as payments to an individual to secure or expedite the performance of a routine government action by government officials) are no exception to the general rule and therefore prohibited.

### **4.2 Anti-Competitive:**

We are committed to conducting our business in a manner that encourages fair and open competition. Anti-Competition means behaviour that aims to reduce competition in the market:

- Fixing prices of services among the competitors within the domestic or international market;
- Rigging bids among competitors in order to enable a competitor to win the bid;

**Prepared By:**



**Ms. Kavita Jain**  
**(DGM-HR)**  
**Date: 01/04/2025**  
Rev. No. 00

**Approved By:**



**Mr. Anurag Hitkari**  
**(Managing Partner)**  
**Date: 01/04/2025**  
Page 6 of 26

## **BUSINESS ETHICS POLICY**

- Allocation of the geographic market among competitors for the purpose of doing business;
- Unlawful exclusivity arrangements among entities that encourage monopolization; and
- Unlawful mergers and acquisitions among companies.

Our Expectation from our People and Partners Worley employees and partners are prohibited from engaging in any activity that promotes unlawful anticompetitive behaviour.

For example, when our employees or partners attend trade or industry forums, we require them to be diligent in all dealings with any competitors and to be aware that talking about prices may be anticompetitive.

In addition, in instances, where our customers engage us to conduct procurement for them, we also comply with all rules relating to prevention of anti-competition.

Prevention of Anti-Competitive Practices: Our Anti-Competition programme consists of the following elements:

- Consideration of anti-competition risks when exploring new business opportunities;
- Ensuring adequate policies and procedures are formulated;
- Investigating allegations relating to anti-competitive behaviour and taking appropriate action accordingly;
- Communicating the message of fair and open competition to the business.

### **4.3 Information Security Management:**

**Prepared By:**



**Ms. Kavita Jain**  
**(DGM-HR)**  
**Date: 01/04/2025**  
Rev. No. 00

**Approved By:**



**Mr. Anurag Hitkari**  
**(Managing Partner)**  
**Date: 01/04/2025**  
Page 7 of 26

## **BUSINESS ETHICS POLICY**

To use all reasonably practicable measures to ensure that:

- Information will be protected against unauthorised access
- Confidentiality of information is assured
- Integrity of information is maintained
- Regulatory and legislative requirements will be met
- Where necessary Business Continuity plans will be produced, maintained and tested
- The rights of all data subjects are protected at all times
- We are able to respond to requests from data subjects professionally and courteously.

The following to be applied as appropriate to our organisation:

- Confidentiality of all company data is to be maintained through discretionary and mandatory access controls
- External service access is restricted to authorised personnel only
- Access to data on all laptop computers is to be secured through encryption or other means to provide confidentiality of company data in the event of loss or theft of company equipment
- Only authorised software may be installed
- The use of unauthorised software is prohibited. In the event of unauthorised software being discovered it will be removed immediately
- Data may only be transferred for approved purposes
- All removable media from external sources must not be attached to our computer equipment unless prior approval is granted

**Prepared By:**



**Ms. Kavita Jain**  
**(DGM-HR)**  
**Date: 01/04/2025**  
Rev. No. 00

**Approved By:**



**Mr. Anurag Hitkari**  
**(Managing Partner)**  
**Date: 01/04/2025**  
Page 8 of 26

## **BUSINESS ETHICS POLICY**

- Passwords must consist of a mixture of at least 8 alphanumeric characters
- The physical security of computer equipment will conform to company requirements
- To prevent the loss of availability of company IT resources measures must be taken to backup data, applications and the configurations of all workstations.
- **Zero incident of information security breaches.**

### **4.3.1 Company approach to Data Protection:**

We aim to conduct our business in compliance with the relevant data protection laws and regulations, including, but not limited to the General Data Protection Regulation. All managers are responsible for implementing the Policy within their areas, and for adherence by their staff. Staff should report breaches of information security, actual or suspected, to their manager. Breaches of the security policies will be investigated in accordance with the company's HR procedures.

### **4.3.2 Data Breach and Reporting:**

In the event, when a reportable data breach occurs and residents are affected, we shall report it to the competent supervisory authority in accordance with the national data protection laws. In case the data breach affects we shall report it to the competent authority in the respective Member States.

### **4.3.3 Cyber Essentials:**

Our policy is based on implementation and ongoing management of the Cyber Essentials framework across the organisation as a minimum.

### **4.3.4 Farewell:**

**Prepared By:**



**Ms. Kavita Jain**  
**(DGM-HR)**  
**Date: 01/04/2025**  
Rev. No. 00

**Approved By:**



**Mr. Anurag Hitkari**  
**(Managing Partner)**  
**Date: 01/04/2025**  
Page 9 of 26

## **BUSINESS ETHICS POLICY**

We will ensure an appropriate firewall is in place to protect our internet connection A boundary firewall and/or personal device firewall will be installed.

### **4.3.5 Devices:**

We will ensure the highest level of security setting on all devices (PC/Laptops, mobile phones, tablets, CCTV). We will remove devices and services we do not use from the network. We will use appropriate user access / password controls. We will use 2 factor authentication for email accounts which process sensitive data.

### **4.3.6 Access Control:**

We will establish appropriate access control processes and mechanisms. We will only use licensed software and devices. Virus and Malware Protection. We will install appropriate virus and malware protection mechanisms.

Users will only be given sufficient rights to all systems to enable them to perform their job function. User rights will be kept to a minimum at all times. Where possible no one person will have full rights to any system. Access to the network/servers and systems will be by individual username and password. Usernames and passwords must not be shared by users. Usernames and passwords should not be written down. Intrusion detection will be implemented where considered necessary and/or at the request of our clients. Users will be given a username and password to login to systems, servers, applications as appropriate. We will be notified of all employees leaving the company's employment. We will then remove the employees' rights to all systems. Network/server supervisor passwords and system supervisor passwords will be stored in case of an emergency. Use of the admin usernames on systems are to be kept to a minimum. Default passwords on systems and other resources will be changed after installation.

**Prepared By:**



**Ms. Kavita Jain**  
**(DGM-HR)**  
**Date: 01/04/2025**  
Rev. No. 00

**Approved By:**



**Mr. Anurag Hitkari**  
**(Managing Partner)**  
**Date: 01/04/2025**  
Page 10 of 26

## **BUSINESS ETHICS POLICY**

### **4.3.7 Updates:**

We will ensure software and devices are updated regularly.

### **4.3.8 Virus Protection:**

Care should be taken when using USB or other types of media brought in from outside the company. Management strongly endorse the company's anti-virus policies and will make the necessary resources available to implement them. Users will be kept informed of current procedures and policies. Users will be notified of virus incidents. Employees will be accountable for any breaches of the company's antivirus policies. Antivirus policies and procedures will be reviewed regularly. In the event of a possible virus infection the user must inform management immediately. Arrangements will be made to scan the infected machine and any servers or other workstations to which the virus may have spread and eradicate it.

### **4.3.9 Physical LAN Security, Hubs/Switches LAN (Local area network)**

equipment, hubs, bridges, repeaters, will be secure.

### **4.3.10 Work Stations:**

All unused workstations must be switched off outside working hours. Users must comply with the terms of our Bring Your Own Device police where applicable Servers [including cloud services]. All cloud storage will be made securely with all appropriate measures taken to ensure data is protected, backed-up, and safe at all times.

### **4.3.11 Inventory Management:**

Managers will keep a full inventory of all computer equipment and software in use throughout the company.

### **4.3.12 Internet Security:**

**Prepared By:**



**Ms. Kavita Jain**  
**(DGM-HR)**  
**Date: 01/04/2025**  
Rev. No. 00

**Approved By:**



**Mr. Anurag Hitkari**  
**(Managing Partner)**  
**Date: 01/04/2025**  
Page 11 of 26

## **BUSINESS ETHICS POLICY**

Connections to the Internet will be via the means of a firewall to regulate network traffic.

### **4.3.13 Email Security:**

If an email is received from an unknown source and you are unsure of its legitimacy, then delete it and please inform your manager. When you start to type in the name of the recipient, email software will suggest similar addresses you have used before. If you have previously emailed several people, whose name or address starts the same way - e.g. "Dave" - the auto- complete function may bring up several "Daves". Make sure you choose the right address before you click send. If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone. When forwarding emails ensure that company privacy is protected at all times, especially when forwarding a chain of emails. Email should always be constructed in a professional manner as the email you are sending is representing the company and the brand the recipient could forward that email onto another party. When sending company data, you must avoid doing so in an anti-competitive way. This includes but is not limited to, price fixing, restricting competitors selling your product, bid rigging, failure to abide by this rule will be dealt with through the disciplinary system.

### **4.3.14 Data Storage:**

**Prepared By:**



**Ms. Kavita Jain**  
**(DGM-HR)**  
**Date: 01/04/2025**  
Rev. No. 00

**Approved By:**



**Mr. Anurag Hitkari**  
**(Managing Partner)**  
**Date: 01/04/2025**  
Page 12 of 26

## **BUSINESS ETHICS POLICY**

All data and information collected and processed in any form (paper, electronic etc.) shall be subject to the requirements of this policy. Any regulation in respect to collection, processing, protection and retention of data/information and such documents shall be stored in a safe place as designated by the company for a retention period provided for by applicable laws and/or indicated by the company. Employees are not permitted to keep any confidential information on mobile devices except information which is temporarily needed for specific, work-related activity. Any download of such files to local devices should be avoided or limited only to necessity related with information processing for work purposes Internet access and operations performed by employees according to the requirements of the applicable laws and regulations may be filtered and monitored by duly authorised IT personnel of or on behalf of the company. Any mobile, portable devices (including laptops, tablets, smartphones and other handheld computing devices) as well as any cloud information storage places should be approved by the company and secured to prevent unauthorised access. Only systems and program software licensed and authorised by the company can be installed and used on equipment and tools used within the company. Before downloading or installing any software to devices held and used by employees for the purposes described in this policy permission from the management team shall be obtained. In cases when employees use home devices the employees shall be obliged to comply with the requirements of this policy; equally as if they were using equipment provided by the company. Accordingly, it shall be prohibited to store any data and information related to the company on the device; any processing of the data shall be permitted only through cloud and online storage places used by the company. In case

**Prepared By:**



**Ms. Kavita Jain**  
**(DGM-HR)**  
**Date: 01/04/2025**  
Rev. No. 00

**Approved By:**



**Mr. Anurag Hitkari**  
**(Managing Partner)**  
**Date: 01/04/2025**  
Page 13 of 26

## **BUSINESS ETHICS POLICY**

access is granted to the employee to a system of a client or cooperation partner of the company; the employee shall be obliged to use the access tools provided by the client or partner and follow provided guidelines on secure information/data processing requirements (including use of encryption systems, passwords, data use limitations, using dedicated locations etc.). No information/data referred to in this policy shall be sent, forwarded or otherwise submitted to any third party, unless it is necessary for the accomplishment of work duties of the employee. In the case of forwarding and submission of data to third parties, it shall be ensured that the data is protected and corresponding security measures have been taken. The company shall audit the systems used in the processing of information/data to control ongoing compliance with this policy and applicable statutory requirements.

### **4.3.15 Data Retention Schedule:**

We will retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons why that personal data was obtained, but should be determined in a manner consistent with our data retention guidelines. For more information, refer to the data retention and erasure policy document.

### **4.3.16 Encryption and Anonymization Data:**

Encryption protects information stored on mobile and static devices and in transmission. It is a way of safeguarding against unauthorised or unlawful processing of data. There are a number of different encryption options available. Anonymization of personal data should be considered where possible and desirable. Anonymization ensures the availability of rich data resources, whilst protecting individuals' personal

**Prepared By:**



**Ms. Kavita Jain**  
**(DGM-HR)**  
**Date: 01/04/2025**  
Rev. No. 00

**Approved By:**



**Mr. Anurag Hitkari**  
**(Managing Partner)**  
**Date: 01/04/2025**  
Page 14 of 26

## **BUSINESS ETHICS POLICY**

data. The company will consider encryption alongside other technical measures, taking into account the benefits and risks that it can offer. Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage to personal data.

### **4.3.17 Prohibited Activities:**

Save for exceptions specifically established; in no case and under no circumstances should any equipment, systems or tools owned by the company, its clients or cooperation partners be used for purposes not related to work duties of the employee or not related to business operation of the company.

The Following Activities Are Prohibited, With No Exceptions:

- Breach of this policy can lead to disciplinary action and other legal action.
- Violation of the rights of any person by excessive and unnecessary collection and processing of personal data.
- Accessing data, storage or an account for a purpose other than conducting business operation or performance of work duties of the particular employee
- Exporting company information in breach of applicable international or national laws and regulations and/or directions.
- Exporting of any data or information which is of proprietary and/or confidential value to the company, if such exporting is not required in the course of business operation performance of work duties of the employee and/or is in breach of internal regulations of the company, applicable laws or regulations.

**Prepared By:**



**Ms. Kavita Jain**  
**(DGM-HR)**  
**Date: 01/04/2025**  
Rev. No. 00

**Approved By:**



**Mr. Anurag Hitkari**  
**(Managing Partner)**  
**Date: 01/04/2025**  
Page 15 of 26

## **BUSINESS ETHICS POLICY**

- Revealing an employee's account password to others and allowing the use of such account by others (including but not limited to employee's family members).
- Effecting security breaches or disruptions of network communication. Such security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account which the employee is not expressly authorised to access, unless such access rights are granted to the employee due to him/her being involved in a specific project of the company.

### **4.3.18 Reporting Security Incidence:**

All information/data processing security incidents or threatened incidents shall be immediately reported to management, which accordingly shall take all measures for prevention of potential damage, elimination of the damage caused and restitution of previous security status. If applicable, it shall be the obligation of the management to ensure further reporting on data/information security breach to all relevant authorities and individuals involved as provided for by applicable laws and regulations.

### **4.4 Anti-Money Laundering:**

The Pragmetis Pharmactives LLP. shall endeavour at all times to comply, in letter and spirit, with the provisions of all relevant laws, rules, regulations, guidelines and circulars issued by regulatory authorities in relation to anti-money laundering and our policies. To these ends the Company shall:

- Establish appropriate 'Customer Due Diligence Process' for:

**Prepared By:**



**Ms. Kavita Jain**  
**(DGM-HR)**  
**Date: 01/04/2025**  
Rev. No. 00

**Approved By:**



**Mr. Anurag Hitkari**  
**(Managing Partner)**  
**Date: 01/04/2025**  
Page 16 of 26

## **BUSINESS ETHICS POLICY**

- Identification of clients (and actual beneficial owners) and verification of their identity;
- Obtaining additional ‘know your client’ information as appropriate and necessary;
- Acceptance of clients;
- Identification of suspicious transactions and reporting of the validated suspicions to the appropriate authorities as required;
- Maintain appropriate records of customer identification and trail of transactions; and
- Co-operate with the regulatory authorities to the extent required by the applicable laws and provide information as may be required, without breaching the customer confidentiality agreement;
- Give appropriate training to the relevant staff for effective implementation of the Policy & Procedures.
- Prevent and deter the use of the Pragmetis Pharmactives LLP. services by money launderers or those involved in criminal activities including financing of terrorism and to protect the reputation of the Company.
- Protect the Company and its employees against unfounded allegations of facilitating money laundering and terrorist financing; and,
- Protect the Company and its employees against any criminal, civil and regulatory actions which might result from inadvertent involvement in money laundering and/or terrorist financing or from failure in operational controls.

**Prepared By:**



**Ms. Kavita Jain**  
**(DGM-HR)**  
**Date: 01/04/2025**  
Rev. No. 00

**Approved By:**



**Mr. Anurag Hitkari**  
**(Managing Partner)**  
**Date: 01/04/2025**  
Page 17 of 26

## **BUSINESS ETHICS POLICY**

### **4.5 Conflict of Interest:**

Conflict of interest includes situations:

- Where an employee's private affairs or financial interests are in conflict with his/her work duties, responsibilities and obligations, or results in a perception that a conflict exists.
- That could impair the employee's ability to act in the Company's interest.
- Where the actions of an employee would compromise or undermine the trust of stakeholders.
- **100% employee should be undergoing awareness training regarding conflict-of-interest topic.**
- A conflict of interest, actual or potential, arises where, directly or indirectly an employee:
  1. proposes to engage in a personal business transaction or a personal relationship with the business associates of our Company;
  2. is offered/derives undue benefit, personally or for, any person with whom he/she has close personal relationship, by making or influencing decisions relating to any transaction;
  3. is in a position to influence a decision with regard to the company's business with a business associate where person with whom he/she has close personal relationship is a proprietor/ director/ partner or representative;
  4. Is in a position to influence decisions with regard to award of benefits such as increase in salary or other remuneration, posting, promotion or recruitment of

**Prepared By:**



**Ms. Kavita Jain**  
**(DGM-HR)**  
**Date: 01/04/2025**  
Rev. No. 00

**Approved By:**



**Mr. Anurag Hitkari**  
**(Managing Partner)**  
**Date: 01/04/2025**  
Page 18 of 26

## **BUSINESS ETHICS POLICY**

a person with whom he/she has close personal relationship, employed in the company.

### **4.6 Fraud Prevention:**

The policy will ensure and provide for the following: -

- To ensure that management is aware of its responsibilities for detection and prevention of fraud and for establishing procedures for preventing fraud and/or detecting fraud when it occurs.
- To provide a clear guidance to employees and others dealing with PRAGMETIS PHARMACTIVES LLP. for bidding them from involvement in any fraudulent activity and the action to be taken by them where they suspect any fraudulent activity.
- To conduct investigations into fraudulent activities.
- To provide assurances that any and all suspected fraudulent activity will be fully investigated.

**4.6.1 Actions constituting fraud:** While fraudulent activity could have a very wide range of coverage, the following are some of the act, which constitute fraud. The list given below is only illustrative and not exhaustive: -

- i. Forgery or alteration of any document or account belonging to the Company
- ii. Forgery or alteration of cheque, bank draft or any other financial instrument etc.
- iii. Misappropriation of funds, securities, supplies or others assets by fraudulent means etc.

**Prepared By:**



**Ms. Kavita Jain**  
**(DGM-HR)**  
**Date: 01/04/2025**  
Rev. No. 00

**Approved By:**



**Mr. Anurag Hitkari**  
**(Managing Partner)**  
**Date: 01/04/2025**  
Page 19 of 26

## **BUSINESS ETHICS POLICY**

- iv. Falsifying records such as pay-rolls, removing the documents from files and /or replacing it by a fraudulent note etc.
- v. Wilful suppression of facts/deception in matters of appointment, placements, submission of reports, tender committee recommendations etc. as a result of which a wrongful gain is made to one and wrongful loss is caused to the others.
- vi. Utilizing Company funds for personal purposes.
- vii. Authorizing or receiving payments for goods not supplied or services not rendered.
- viii. Destruction, disposition, removal of records or any other assets of the Company with an ulterior motive to manipulate and misrepresent the facts so as to create suspicion/suppression/cheating as a result of which objective assessment/decision would not be arrived at.
- ix. Any other act that falls under the gamut of fraudulent activity.

### **4.7 Whistle Blower Policy:**

#### **4.7.1 Preamble**

Section 177 of the Companies Act, 2013 requires that the Company shall establish a vigil mechanism for directors and employees to report concerns about unethical behaviours, actual or suspected fraud or violation of the company's code of conduct or ethics policy. This mechanism should also provide for adequate safeguards against victimization of Directors / Employees who avail the mechanism and also provide for direct access to the Committee in exceptional cases.

**Prepared By:**



**Ms. Kavita Jain**  
**(DGM-HR)**  
**Date: 01/04/2025**  
Rev. No. 00

**Approved By:**



**Mr. Anurag Hitkari**  
**(Managing Partner)**  
**Date: 01/04/2025**  
Page 20 of 26

## **BUSINESS ETHICS POLICY**

Accordingly, the Whistle Blower Policy (“the Policy”) has been formulated with a view of provide a mechanism for the Directors / Employees of the Company to approach the designated persons / Committee of the Company to, inter alia, report to the management instances of unethical behaviour, actual or suspected, fraud or violation of the company’s code of conduct or policy.

### **4.7.2 Purpose**

To provide Directors / Employees, supplier, customers to raise concerns to the highest possible standards of ethical, moral and legal business conduct and its commitment to open communication and to provide necessary safeguards for protection of associates from victimization, for whistle blowing.

### **4.7.3 Applicability**

The policy is applicable indiscriminately to all Partner / Employees, customers, suppliers & Other stakeholders.

### **4.7.4 Important Features of the Policy**

The whistle blowing policy is intended to cover serious concerns that could have a large / material impact on the company such as:

- I. Corruption & Bribery Reporting
- II. Information Security Birches
- III. Discrimination & Harassment Issue
- IV. Suspected action,
- V. Incorrect financial reporting,
- VI. Actions which are not in line with the Company’s policy, (iv) unlawful actions,

**Prepared By:**



**Ms. Kavita Jain**  
**(DGM-HR)**  
**Date: 01/04/2025**  
Rev. No. 00

**Approved By:**



**Mr. Anurag Hitkari**  
**(Managing Partner)**  
**Date: 01/04/2025**  
Page 21 of 26

## **BUSINESS ETHICS POLICY**

VII. Fraud

VIII. Food Safety, Quality and Legality.

IX. Any other actions which are not legal and will have an impact on the performance and image of the Company.

### **4.7.5 Complainant**

Partner, Employees, customers, suppliers, stakeholders of the Company (“Complainant / Whistle-blower”). The complainant needs to demonstrate to the Company, that there are sufficient grounds for concern.

### **4.7.6 Protection**

1. Harassment or victimization of the complainant will not be tolerated.

2. Confidentiality.

Every effort will be made to protect the complaint’s identity, subject to legal constraints.

3. Anonymous Allegations

Complainants need to mention their names to allegations. Normally, anonymous complains will not be investigated. However, the same will be investigated subject to seriousness of the issue raised.

4. Malicious Allegations

5. After the investigation, if it is found that it was a malicious allegation by the complainant, the same will result into disciplinary action.

### **4.7.7 Authority**

The investigation authority will be a person or group of persons of the Company constituted for the investigation of the complaints.

**Prepared By:**



**Ms. Kavita Jain**  
**(DGM-HR)**  
**Date: 01/04/2025**  
Rev. No. 00

**Approved By:**



**Mr. Anurag Hitkari**  
**(Managing Partner)**  
**Date: 01/04/2025**  
Page 22 of 26

## **BUSINESS ETHICS POLICY**

The Company could also appoint an outside agency for investigation of the matter.

### **4.7.8 Reporting**

The whistle blowing procedure is intended to be used for serious and sensitive issues. Serious concerns relating to financial reporting, unethical or illegal conduct should be reported to the Investigating Authority.

The Complaints can be reported to the following persons in writing through suggestion box mail & mobile no:

|                                       |                |
|---------------------------------------|----------------|
| Managing Partner - Mr. Anurag Hitkari |                |
| hitkari@pragmetis.com                 | +91 9998141951 |
| DGM-Human Resources – Ms. Kavita Jain |                |
| hr@pregmetis.com                      | +91 8696204205 |

### **4.7.9 Investigation**

All complaints received will be recorded. If initial enquiries by the Investigating Authority reveals that the Complainant has no basis, it may be dismissed at this stage. Where initial enquiries indicate that further investigation is necessary, this will be carried through Investigating Authority or it may engage an outside agency for the said purpose. The investigation would be conducted in a fair manner. The principles of natural justice and equity will be followed. A written report of the findings will be made. After the investigation if the Compliant is proved, disciplinary action including dismissal will be considered.

If the complaint is false or malicious, suitable action like fine or dismissal will be considered.

**Prepared By:**



**Ms. Kavita Jain**  
**(DGM-HR)**  
**Date: 01/04/2025**  
Rev. No. 00

**Approved By:**



**Mr. Anurag Hitkari**  
**(Managing Partner)**  
**Date: 01/04/2025**  
Page 23 of 26

## **BUSINESS ETHICS POLICY**

The Report the complaints received, outcome of the investigation will be given to the Whole-time Partner of the Company.

### **4.7.10 Communication**

The complaint received from the complainant will be acknowledged. If additional information is required, the Investigation Agency will contact the complainant to get additional information. The outcome of the investigation will be communicated to the complainant.

### **4.7.11 Flexibility**

This policy can be changed, modified, rescinded or abrogated at any time by the Company.

### **4.7.12 Complainants' Responsibilities**

To bring early attention of the company any improper practice they become aware of. Co-operate with investigating authorities, maintaining full confidentiality. A complainant has the right to protection from retaliation.

If the Complainant is not satisfied with the outcome of the investigation, the complainant can take up the matter with the Committee.

### **4.7.13 Role of Investigation Authority**

It is ensured that the policy is being implemented. Ascertain prima facie the credibility of the charge. If initial enquiry indicates further investigation is not required, close the issue. Document the initial enquiry. Provide quarterly report to the Partner of the Company. Acknowledge receipt of concern to the complainant. Ensure that necessary safeguards are provided to the complainant. Conduct the enquiry in a fair, unbiased manner. Ensure complete fact-finding. Maintain strict confidentiality. Decide on the

**Prepared By:**



**Ms. Kavita Jain**  
**(DGM-HR)**  
**Date: 01/04/2025**  
Rev. No. 00

**Approved By:**



**Mr. Anurag Hitkari**  
**(Managing Partner)**  
**Date: 01/04/2025**  
Page 24 of 26

## **BUSINESS ETHICS POLICY**

outcome of the investigation. Recommend an appropriate course of action including dismissal, and preventive measures. Minute Committee deliberations and document in the final report.

### **4.7.14 Action Taken Report**

The whole-time director shall place before the Board quarterly reports of the Investigating Agency and ensure necessary action is taken based on the report of the Investigating Agency.

We are committed to comply with all applicable laws and regulatory requirements concerning our operations in the jurisdictions which the company operates.

This policy shall be reviewed periodically for its suitability and updated as necessary.

### **4.8 Approval Procedure for Sensitive Transaction**

Sensitive transactions are usually in the nature of kickbacks, gifts of significant value, bribes or pay offs made to favorably influence some decision affecting a company's business or for the personal gain of an individual.

- All transactions should comply with applicable laws.
- Pregmetis policy prohibits the company and its employees and agents from corruptly offering or giving anything of value to political party/government officials inside/outside the India or an official of a public international organization.
- Sensitive transactions may be direct or indirect, for the purpose of influencing officials in their official capacity or in violation of their lawful duties or to secure any improper advantage in order to help the company obtain or retain business or direct business to any person.

**Prepared By:**



**Ms. Kavita Jain**  
**(DGM-HR)**  
**Date: 01/04/2025**  
Rev. No. 00

**Approved By:**



**Mr. Anurag Hitkari**  
**(Managing Partner)**  
**Date: 01/04/2025**  
Page 25 of 26

## **BUSINESS ETHICS POLICY**

- Pregmetis Corporation policy prohibits any employee or agent from making any payment or engaging in any transaction that is prohibited by the law.
- Establish the process necessary to deliver the results in accordance with the requirements and implement the process to ensure proper handling of sensitive transactions.
- Monitor and measure the process against the requirement and take actions to continually improve the system.

**Next review on 31<sup>st</sup> March 2026.**

**Prepared By:**



**Ms. Kavita Jain  
(DGM-HR)  
Date: 01/04/2025  
Rev. No. 00**

**Approved By:**



**Mr. Anurag Hitkari  
(Managing Partner)  
Date: 01/04/2025  
Page 26 of 26**