1. Introduction

DSP Asset Managers Private Limited (hereinafter referred to as "DSPAM") maintains a reputation for conducting its business and business activities in the highest professional manner consistent with our values and principles. No matter what your role is, or which location you work in, you are expected to:

- Demonstrate the behaviours of honesty, integrity, quality, and trust at all times.
- Be a role model and recognize those around you who also demonstrate these behaviours.
- Speak out when you feel these behaviours are threatened or compromised.

To aid in this objective, DSP has several policies and guidelines that assist you in maintaining these standards.

The purpose of the Whistle Blower Policy ("the Policy") is to encourage you to report matters without the risk of subsequent victimisation, discrimination, or disadvantage. The Policy applies to all employees working for DSPAM and its subsidiaries as follows:

A. DSP Pension Fund Managers Private Limited
B. DSP Fund Managers IFSC Private Limited

The Whistle Blowing or reporting mechanism set out in the policy, advises all employees to act responsibly to uphold the reputation of DSP. The policy aims to provide a mechanism to ensure that concerns are properly raised, appropriately investigated, and addressed.

2. Definition

2.1 Audit and Risk Committee

Audit and Risk Committee ("the Committee") constituted by the Board of Directors of DSPAM.

2.2 Employee

Every bonafide employee currently in the employment of DSPAM and its subsidiaries. For the purpose of this policy, employee also includes directors of DSPAM, its subsidiaries.

2.3 Whistle Blowing Redressal Committee

Whistle Blowing Redressal Committee shall comprise the following Company officials i.e. Head-Human Resources, Head- Legal & Compliance and Chief Risk Officer.

2.4 Retaliation / Victimisation

Retaliation refers to any act, whether direct or indirect, recommended, threatened, or taken against a whistleblower as a result of their disclosure made in accordance with the policy. It includes various forms of overt or covert acts aimed at causing harm or negative consequences to the whistleblower.

These acts can include:

Discrimination: Treating the whistleblower unfairly or differently based on their status as a whistleblower, such as denying promotions, salary increases, or training opportunities.

Reprisal: Taking retaliatory actions against the whistleblower, such as demotion, transfer to less desirable positions, or adverse changes in work assignments.

Harassment: Subjecting the whistleblower to unwelcome or hostile behaviour, including verbal abuse, intimidation, threats, or creating a hostile work environment.

Vengeance: Engaging in vindictive actions to harm the whistleblower, such as spreading false rumours, damaging their reputation, or taking personal or professional actions to cause distress or harm.

2.5 **Whistle Blower**

A Whistle Blower means any employee who raises a concern in accordance with this Policy.

2.6 Whistle Blowing 'Concern' or 'Complaint'

Whistle blowing (also referred to as 'complaint' or 'concern') can be described as attracting management's attention to information about potentially harmful, illegal and/or unacceptable practices.

Employees can raise concerns/issues, if any, which they have on the following or possibilities/apprehensions of:

- Breach of any law, statute or regulation by DSPAM & its subsidiary
- Issues related to accounting policies and procedures adopted for any area or item.
- Acts resulting in financial loss or loss of reputation.
- Misuse of office, suspected/actual fraud and criminal offences.
- Instances of leak or suspected leak of Unpublished Price Sensitive Information ('UPSI').
- Identification & deterrence of market abuse including front-running and fraudulent transactions in securities
- Any other issue which can cause significant harm to individual / organization's wellbeing.

3. **Reporting of a Whistle Blower Concern/Complaint**

3.1 The employee may send a communication directly in writing through a letter or by e-mail to whistleblower@dspim.com or to any member of the Whistle Blowing Redressal Committee of DSP.

3.2 The whistle blower (i.e. employee or director making the complaint) is encouraged to provide the following information in his/her complaint: name, contact details if any, and department.

3.3 Other than complaints relating to concerns regarding questionable accounting or auditing matters, DSP shall not entertain any complaint where information mentioned in 3.2 is not provided, including anonymous/pseudonymous complaints.

3.4 In respect of such anonymous/pseudonymous complaints (i.e. other than complaints relating to concerns regarding questionable accounting or auditing matters), no further action will be required to be taken and the case will be closed, without intimation to the complainant.

3.5 The Whistle Blowing Redressal Committee has the authority to exercise discretion and consider anonymous or pseudonymous complaints, even if they are not specifically related to questionable accounting or auditing matters, depending on the circumstances and merits of the complaint.

3.6 Any concern received by the Head of Departments (in writing or through email) shall be forwarded to the Whistle Blowing Redressal Committee for further action. Such concern shall also be considered as a concern received under this Policy and accordingly addressed.

3.7 Within a reasonable time of receipt of the concern by the Whistle Blowing Redressal Committee,

1. An acknowledgment shall be sent to the sender of the concern (where a return address or email address is available.

2. The acknowledgment shall confirm receipt of the concern and inform the sender that the concern would be inquired into, appropriately addressed and reported to the Audit and Risk Committee.

3. In case the concern does not fall within the ambit of the Whistle Blower Policy, the sender shall be informed that the concern is being forwarded to the appropriate department/authority for further action, as may be deemed necessary.

4. Administration of the policy

4.1 The Whistle Blowing Redressal Committee will promptly investigate concerns or complaints received. They will report the details of the concerns to the Audit and Risk Committee during their subsequent quarterly meeting. The Whistle Blowing Redressal Committee will also update the Audit and Risk Committee on the investigation's progress and actions taken. They will follow any directions or guidance given by the Audit and Risk Committee if any for further action.

4.2 The Whistle Blowing Redressal Committee will generally complete the investigation of concerns received within 120 days. If a concern requires more time for inquiry, the committee will inform the Audit and Risk Committee during the quarterly reporting of the inquiry's progress. Once the investigation is finished, the committee will communicate any actions to be taken by the relevant departments within DSPAMC and track the closure of those actions. A concern will remain open until the necessary actions are initiated or completed.

4.3 Once the inquiry is concluded, the concern will be considered closed. This closure can happen when disciplinary action is taken, recovery proceedings are initiated, external legal proceedings are commenced, or when reporting requirements under applicable laws and policies are fulfilled. The closure of the concern will be reported in the subsequent quarterly meeting of the Audit and Risk Committee.

4.4 The Whistle Blowing Redressal Committee will provide a quarterly report to the Audit and Risk Committee, which will include the status of all open concerns. Additionally, concerns that were closed during the previous quarter will also be communicated to the Audit and Risk Committee, along with relevant details.

5.Protection to employees and prevention against retaliation, victimisation or harassment of employees raising any concern under the Policy.

5.1 Employees who make a disclosure or raise a concern under the Policy will be protected if they meet the following criteria:

1.Good Faith: The employee discloses the information in good faith, meaning they genuinely believe that the concern they are raising is valid and important.

2.Substantial Truth: The employee believes that the disclosed information is substantially true, indicating that they have reasonable grounds and evidence to support their concern.

3.Non-Malicious Intent: The employee does not act maliciously or make false allegations. This implies that their disclosure is not driven by ill will or a desire to harm others, and they provide truthful information to the best of their knowledge.

4. No Personal or Financial Gain: The employee does not seek any personal or financial benefit from DSPAMC (the organization). This ensures that their motive for disclosure is focused on the well-being of the organization and its stakeholders rather than personal gain.

By meeting these criteria, employees who make disclosures or raise concerns will receive protection under the Policy.

5.2 DSPAM will not tolerate retaliation against employees who report genuine concerns of wrongdoing.

5.3 Protection under the Policy is available to employees who raise concerns as long as their employment with DSPAM continues.

5.4 Employees can report concerns regarding disciplinary action or retaliation within three months of the incident.

5.5 The Whistle Blowing Redressal Committee may consider concerns raised beyond the three- month period under its discretion.

5.6 Any attempt by an employee to misuse the policy for personal gain will be strictly dealt with by DSPAM.

5.7 Right to Seek Monetary Awards: The policy does not prevent complainants from seeking monetary awards provided by law from government, administrative, or law enforcement authorities.

5.8 The policy does not excuse employees from compliance with DSPAM's Code of Conduct or other internal policies. Violations of these may result in separate proceedings and actions by DSPAM, distinct from the provisions of this Policy.

5.9 The provisions of the Policy remain intact for employees who raise concerns in good faith, as determined by the Whistle Blowing Redressal Committee.

5.10 Employees who are not considered whistleblowers, either due to their acts or omissions, are not entitled to the protections provided by the Policy.

5.11 Employees are requested to go through 'Policy on protection of Whistleblowers' to have a clear and predeterminate procedure for reporting of any actual or suspected leak of UPSI, and are duly protected once such leakage is suspected or has taken place.

6. Confidentiality and Anonymity

6.1 Employees can choose to submit complaints anonymously or using a pseudonym for matters related to questionable accounting or auditing. However, it is encouraged to disclose their identities to assist with obtaining necessary details or evidence during the investigation.

6.2 The identity of the complainant will be kept confidential during and after the investigation, unless required by law.

6.3 If an employee discloses their identity, they will still receive protection as defined in Paragraph 5 of the Policy. Their employment-related matters, such as performance appraisal and work assignments, will not be affected.

6.4The Policy does not prevent IPAMC from taking appropriate action against an employee who improperly discloses the complaint, violates the Code of Conduct, or publicly shares the fact that they lodged the complaint.

6.5 Such proceedings and actions taken by IPAMC are separate from the provisions of the Policy. However, if it is determined by the Audit and Risk Committee or the Whistle Blowing Redressal Committee that the employee blew the whistle in good faith, the protections of the Policy still apply.

7. Record Keeping

Records pertaining to the complaint shall be maintained by the Human Resource Department (HRD) as per Preservation of Documents Policy of IPAMC.

Annexure – 1

List of members of Whistle Blowing Redressal Committee

Sanjiv Kumar
Head - Human Resources
25th Floor, The Ruby, 29, Senapati Bapat Marg, Dadar West, Dadar, Mumbai, Maharashtra 400028
Email: sanjiv.kumar@dspim.com

Pritesh Majmudar
Head – Legal & Compliance
25th Floor, The Ruby, 29, Senapati Bapat Marg, Dadar West, Dadar, Mumbai, Maharashtra 400028
Email: pritesh.majmudar@dspim.com

Pranjal Vora
Chief Risk Officer
25th Floor, The Ruby, 29, Senapati Bapat Marg, Dadar West, Dadar, Mumbai, Maharashtra 400028
Email: pranjal.vora@dspim.com