Surveillance Policy And Monitoring of Transactional Alerts

Back Ground :

Inani Securities Limited has framed this policy for strengthening the surveillance frame work to facilitate effective trade surveillance operations, identify common types of market abuse practices and provide accountability matrix for different types of suspicious behavior thus protecting the system from unlawful money and activities entering into the system. To Monitor and report the Suspicious Transactions, if any to FIU IND. And to be in compliance with SEBI, AML and TFT Provisions.

To be In compliance with SEBI circular (Reference no. SEBI/HO/MIRSD/MIRSD-PoD 1/P/CIR/2024/96 dated July 04, 2024 titled 'Measures to instil confidence in securities market – Brokers' Institutional mechanism for prevention and detection of fraud or market abuse' and NSE circular 'NSE/SURV/62827' dated 8 July 2024.

Implementation standard :

The surveillance alerts generated by our internal and FIN KORP Software system based on the DP and Trading operations, Risk profile, Client Due Diligence and UCC / KYC details of the Clients, the and those provided by the Exchanges, Depositories and other regulators shall be conducted under the overall supervision of compliance officer in coordination with the staff, senior management along with the Principal Officer and the designated Director .

The Surveillance systems and internal controls are built in a manner that are commensurate with the complexity of the transactions done by our clients and our business activities The surveillance alerts generated by our FIN KORP Software system based on the Clients Trading, DP, Demat holdings, funds flow activities, Risk profile, Income Range, Occupation, common demographic details, frequent changes in KYC details, frequent off market Trades, Irrational Pledge transactions, dealing in illiquid shares or derivatives, dealing in concentrated trades, dealing in high values not commensurate with income or occupation, dealing as a group with concentration in specific scrip, unable to establish proper reason or logic on the transactions executed by the client, and any other irrational activities, and UCC / KYC details of the Clients as per our surveillance mechanism shall be continuously monitored on ongoing process by our trained staff under the supervision of Surveillance team, the Principal Officer and the Designated Director.

All our staff and associates are adequately trained to monitor the surveillance of client behavior through analyzing the pattern of trading and DP activities done by our clients, detection of any unusual activity being done by such clients and escalate the suspicious transaction as laid down under the policy to the Surveillance team, the Principal Officer. Appropriate measures will be initiated after verifying the genuineness of the alerts, as per the policies and CDD measures to prevent any kind of fraudulent activity in the market in terms of the regulatory requirements prescribed by SEBI and Market Infrastructure Institutions (MIIs). Any Suspicious transaction shall be reported to the Exchanges,
Depositories, FIU IND and any other regulators as per the PMLA and other policies laid down by the

Company at a period less than 48 hours from the detection of Suspicious transaction without tipping off.

Resources for undertaking Surveillance monitoring and review activity:

The Surveillance team with two senior officials is set up to monitor the Surveillance activities under the supervision of the Principal Officer Mr. Lakshmikanth Inani and the Designated Director,
Mr. Vishnukanth Inani

The Mid and Senior level staff handling KYC and Surveillance Activity including the Principal Officer shall mandatorily complete the NISM e-learning Certification on AML, KYC, CDD and CALM latest by 31/12/2026.

An ongoing employee training programmed shall be conducted to ensure that all the staff are adequately trained in AML/Surveillance obligations and apprising on the surveillance policy. Such training shall be conducted with specific focus on frontline staff, back-office staff, compliance staff, risk management staff and staff dealing with new clients. The said training shall be conducted at least once in a year.

Systems for alert generation:
Commensurate with our business transactions and behavior of our clients to have adequate surveillance systems in place, to customize our surveillance systems and internal controls the alerts are generated by our FIN KORP software internally and by the Depositories and the Exchanges are monitored by our Surveillance team.

Client Screening and Due Diligence:
We shall strictly adhere to the KYC guidelines as prescribed by SEBI, Exchanges, KRA and CKYC. CDD shall be carried on an ongoing basis.

We shall not allow any client to trade unless they have complied with the KYC Guidelines and the KYC is approved by the KRA. All the latest KYC details and information shall be updated to the KRA. Depositories and Exchanges.

We shall be continuously following the SEBI Master circular on AML on client screening and due diligence.

Type of Alerts to be generated and/or reviewed:

Apart from the alerts generated by the Exchanges and the Depositories, We would be generating additional Surveillance alerts based on the analysis of patterns and trends guided by different themes based on certain threshold / parameters which include the criteria/red flag indicators provided by the Exchanges from time to time. The Indicative themes are as annexed :

Type of Alerts to be generated and/or reviewed:

S.No	INDICATIVE THEMES (Trading Related)
1.	Client / group of clients accounting for a significant percentage of the total trading activity in a scrip / contract as compared to the market.
2.	Client / group of clients with new account or clients dealing after a significant time gap, as accounting for significant value / percentage of total trading activity in a scrip / contract as compared to the market.
3.	Client / group of clients dealing frequently in small quantities/minimum market lot in a scrip / contract.
4.	Disproportionate trading activity vs reported income / Net worth.
5.	Frequent changes in KYC submitted by clients.
6.	Based on an announcement by a listed company, Client / group of clients, having possible direct / indirect connection with a listed company, who have undertaken any suspicious trading activity prior to price sensitive announcement by said listed company.
7.	Client / group of clients having significant selling concentration, in the scrips, forming part of 'For Information list' or 'Current Watch list'
8.	Consistency in profit / loss at client / group of clients' levels, rationale for such trading activities.
9.	Significant trading activity in shares by client who has pledged the shares of same scrip.
10.	Trading activity of a client or a group of clients in a scrip, the orders are being placed by respective clients or their authorized representatives and monitoring client's address as per KYC vis-à-vis the dealing office address
11.	Trading activities of accounts of relatives of entity to identify any sort of synchronized / coordinated trading.
12.	Surveillance / monitoring of IP addresses of clients (including identification of multiple client codes trading from the same location)
13.	Client/Group of Client (s), dealing in common Shares/Commodities.
14.	Pump and Dump
15.	Order book spoofing i.e. large orders away from market
16.	Front Running

S.No.	INDICATIVE THEMES (DP Operation Related)
1	Alert for multiple demat accounts opened with same demographic details
2	Email id/address of clients are getting bounced
3	Frequent changes in the details of the demat accounts
4	Frequent Off-Market transfers by a client
5	Off-market transfers not commensurate with the income/Net worth
6	Pledge transactions not commensurate with the income/Networth
7	Off-market transfers (High Value) immediately after modification of details
8	Reason of Off Market transfers not matching with Client profile
9	Sudden Increase in transactions in New accounts
10	Account Opened and Quickly Closed
11	High Volume/ Value Dematerialization Alerts
12	Transaction in Dormant Account
13	High Value Credit/ High Quantum Credit / High value Gift or Donation Credit
14	High Value Debit / High Quantum Debit / High value Gift or Donation Debit
15	High Volume/ Value Preferential Allotment
16	Significant Holding in Listed Scrip
17	High Volume/ Value Off-market transactions in scrip appearing in GSM OR ASM list published by exchanges
18	Others (Transfer of Suspended shares, any other concerns

Apart from the above, we shall have our own thresholds and parameters to generate additional alerts based on transactional activities, payments made or received, nature of off market / on market / pledge transactions of the clients to ascertain whether the transactions are done with own funds for self or on behalf of any other persons and the rationale behind executing such trades to identify the suspicious transactions.
Based on the volume of our business and Clientele, all the Off Market / Pledge transactions are scrutinized by our compliance officer before execution to verify the genuineness of the transaction.

The above review shall also include the alerts generated by the Exchanges And Depositories:

Factors to be considered for generating alerts:

ALERT	DESCRIPTION OF THE ALERT	CRITERIA FOR GENERATING ALERTS
1.	Client / related group of clients has large share of traded volume in a particular security in cash segment	Volume as 30 % of daily exchange volume
2.	Client / related group of clients has a large share of traded volume in contracts of a particular underlying.	Volume as 20% of daily exchange volume.
3.	Client / related group of clients dealing in illiquid shares near the price bands in small quantities.	5 continuous trading Days.
4.	Margin obligations disproportionate to declared income / Net worth (peak of the month)	If more than max 2 times the Net Worth or 8 times the peak of income range.
5.	Net funds pay-in/ pay-out during a period (one month) disproportionate to declared income/ Net worth	If more than max 2 times the Net Worth or 8 times the peak of income range.
6.	Frequent changes in any element of KYC (for mule accounts)	6 times of such changes of same element in an year.
7.	Client / related group of clients having significant selling concentration, in the scrips, forming part of 'For Information list' or 'Current Watch list'(SMS)	Value Exceeding Rs. One Crore
8.	Clients making net profit/ losses over a period which is a significant amount as compared to their income/ Net Worth in cash segment beyond a particular threshold	If more than max 1 time their Net Worth or 2 times the peak of income range.
9.	Order placed by multiple unrelated clients from the same IP/ device in case of internet-based trading clients.	If more than 6 clients.
10.	Repeated failure to deliver securities for pay-in obligations leading to auction/ close out in illiquid items (for reasons other than shortage of payout received in previous settlement)	If more than 4 times in a month
11.	Circular trading/Reversal pattern at same Trading Member above a threshold over a period of 1 month	Where profit / loss is more than Rs. 20 Lakhs.
12.	Front Running by Dealers/Clients to large trades of the Trading Member	Repeated trades by dealer in same security and before order of more than INR 0.50 Crores done in the firm
13.	Substantial proportion of the market open interest in a particular commodity / contract	If more than 5%.

The Principal Officer (PO) / Designated Director (DD) are empowered to decide and alter the thresholds along with documented rationale as per the business needs.

The above review shall also include the alerts generated by the Exchanges and Depositories:

All the Internal / Exchange/Depository alerts shall be reviewed periodically by the Principal Officer at least every 30 days till such time the alert is open.

Obligation on Internal Controls and role of Employees:

All the proprietary trades are made for investments and we shall be executing the same only from our head office Terminal and such trades are executed for the purpose of carrying out proprietary trades only in accordance with the requirements as may be specified by the Board or the stock exchanges from time to time.

All the proprietary trades are reviewed by our Principal Officer / Designated Director on regular basis, the same is reported to the Board at least annually for its review.

Trading Terminals:

Trading terminals are allotted to Branches/HO/Authorised Persons only after updating the details to the Exchanges. We shall continuously monitoring the Login details of the trading terminals to ensure that the terminals are operated by the respective NISM certified Dealers only at the location notified to the Exchanges only and that none of the clients have direct operational access in any manner. The audit team through its intelligence reports by way of monitoring the attendance register/CC TV and surprise visits/random inspections shall ensure the compliance of the same.

To detect and prevent mule/ suspicious Activities as per our **Standard Operating Procedure** (SOP), we shall ensure that Authority to operate trading account is allowed to only family members in case of Individual Accounts and Employees /Group Company Employees/Apex body members - Directors, Partners, Trustees, etc. and Promoter/ Promoter group only, In case of other than Individuals. All such authorizations are allowed on being satisfied and declarations to that effect obtained.

All our Employees/Associated/ Authorised Persons are trained to identifies any fraud, market abuse, suspicious activity and the same shall be immediately to the senior management. We shall be communicating the responsibly of such an obligation to all our Employees /Associated/ Authorised Persons through webinars/ training programs/ written/ mail communication at a period not more than one year.

Escalation and reporting mechanisms:

In order to analyze the trading & DP activities of the Client(s) / Group of Client(s) or scripts identified based on the alerts generated by the Exchanges, Depositories, Regulators and additional surveillance alerts generated by us.

We shall :

a). Analyze and review the alerts based on the facts, transaction rationale and verification of relevant documents including Income / Net worth as provided by the client, further exercise independent judgment by seeking explanation from such identified Client(s) / Group of Client(s) for entering into such

b). Seek documentary evidence such as Bank statement / Demat transaction / Comtrack statement or any other documents to satisfy our self on the said transactions. The period for such statements may be at least +/- 15 days from the date of transactions or as may be required to verify whether the funds / securities for the settlement of such trades actually belongs to the client for whom the trades were transacted.

c). After analyzing the documentary evidences, including the Bank / Demat / Comtrack statement or any other statements, evidences substantiating the cause of action, the cause for such actions shall be recorded. All the observations for such identified transactions will be recorded.

A detailed MIS report with the count of Alerts generated, its status of pendency shall be placed before the Board on **Quarterly basis**, the Board reviews the adequacy and efficiency of the systems for internal control and reporting by analysing the relevant data and initiates appropriate action where ever necessary and approves the same.

Any Suspicious Activity identified and reported to FIU IND as per the policy shall be notified to the Exchange and Depositories along with all the supporting documents immediately but not later than 48 hours from such detection, in such manner as may be specified by the Board or the Stock exchanges/Depositories from time to time. Such information shall be sent NSE via email to Member Surveillance Dashboard (MSD).

We shall submit a summary analysis and action taken report on instances of suspicious activity, fraud and market abuse or a ‘nil report’ where no such instances were detected, on a half-yearly basis to the stock exchanges.

Any deviation in adherence to internal controls, risk management policy, surveillance policy, policy for on boarding of clients along with the proposed corrective actions for such deviation shall be placed before Board of Directors at regular intervals at a period not more than three months and such deviations shall also be reported to the stock exchanges by the Principal Officer / Designated Director.

We shall obtain guidance from the stock exchanges on any suspicious activity which were identified by it, but the violation of the provisions of any applicable law in respect of such activity could not be ascertained due to the limited information available with us, the same shall be communicated to the Exchange.

Guidance on factors to be assessed while reviewing the alerts:

Type of Activity	Factors that are Assessed
Creation of misleading appearance of trading: Trading of a security that occurs at specified prices, volumes and time in a manner agreed upon by the market participants in an attempt to match each other's trades. It may involve a group of clients and/or 'Authorised Persons' acting in concert. Such trading behavior has the effect of creating a false or misleading appearance of active trading in the security.	• Potential connections and relations between clients, based on KYC • Frequency of occurrence and quantity of matched trades that suggest pre-arranged, wash, or circular trading • Market impact, trades of disproportionate volumes • Time proximity of order entries • Thresholds to be determined by brokers as per their business size.
Price manipulation: Trades that have the effect of artificially raising or lowering the market price of a security may create a false market. Greater scrutiny shall be emphasized on shares/commodities which cause significant price movements.	• Unusual price movements • Timing of trades near sensitive periods, such as end of month, quarter, before announcements • Trades causing movements significant price • Thresholds determined as per our policy
Front Running: Trades undertaken while being privy to a big client order	• Time proximity of front running order and big client's order • Same or better price of front running order • Frequency and repeated patterns of occurrence • Abnormal profit pattern
Insider Trading: Trading in securities that are listed or proposed to be listed on a stock exchange when in possession of unpublished price sensitive information.	• Client trading around a material announcement • Abnormal profit pattern • Abnormal trading pattern • Clients connected to Listed Companies • Clients who got huge gains around a material announcement.

Un Authorised Trading: Trades executed in client's account taking instructions on orders from a third party ('Authorised Person' / Member/ any person) with or without the client's prior authorization.	• Authorised Person' with unusual or high volume of error account activities. • Same mobile number /E Mail tagged to different client accounts. • Unusually high number of trading accounts opened / managed under the same person.
Mule Accounts	• Payin obligation / Margin obligation which is disproportionate to reported income / Networth • Same mobile number / email id tagged to different client accounts. • Potential connections and relations between clients, based on KYC.
Pump and dump of securities: A manipulative scheme in which a person or group of persons tries to increase the price of a security using fake information. They do this by using social media and online forums to create a sense of excitement in a security or spread false news about the company's prospects. They then sell (or 'dump') their securities and take a profit, and other security holders suffer as the security price falls.	• Elevated trading activity in small cap/penny scrips. • MIIs and brokers shall have organised social media campaigns with regard to certain securities. • Aggressive purchasing by one or several accounts to have a significant impact on price and encourage other traders to participate in the buying activity. This activity further impacts the price of the underlying security.
Order Spoofing: Places large orders to create the impression of Huge sale or Buy and cancels them on taking advantage of the situation on the Traded/Placed Orders already executed by him and covering the same	• Frequent cancellation or cancellation of large number of orders. • Placement of large orders above or below the prevailing price.

Indicative list of entities who should be surveilled, controls for monitoring, and consequences of potential fraud or market abuse covered are as follows:

Entity being surveilled	Controls for Monitoring	Consequences of potential fraud or market abuse
Client / relatives of client	Trade Surveillance alerts to trace matched trade within such clients to create volume, activity in penny scrip, trading around unusual price movements, frequent cancellation or cancellation of large number of orders etc. Pre-trade controls like blocking of scrips based on assessment /illiquid additional surveillance contracts, margins in volatile scrips/contracts, trade execution range, etc. either at client level or at the scrip level. Monitoring disproportionate trading activity vis-à-vis reported income/net worth, sudden surge in Dormant account / client trading activity/ activity in SMS stocks/ Client concentration in particular scrip etc. Implementing online alerts / nudges. IP address / Device Identification of multiple client codes trading from the same location/device. Monitoring of Trading activity with the declared income / Net worth. Calling and verifying clients on sample basis Email alert on old contact details on change in email id of retail clients. Internal alert for same name and DOB with Multiple PAN at the time of Account opening. Internal Alert for same bank account mapped to multiple clients, controls during account opening to scrub against existing bank details, In-person verification. Same email/phone number mapped to multiple non-family accounts Unusual trading pattern	• Creation of misleading appearing of trading • Front running • Un authorised trading • Insider trading • Order Spoofing • Price Manipulation • Disproportionate trading activity vis-à-vis reported income/net worth • Sudden surge in dormant account • Sudden surge in client trading activity • Activity in SMS stocks • Client concentration in particular scrip • Mule accounts that attempt to conceal malpractices. •Disproportionate trading activity - reported income/net worth • Un authorised trading or Mis- selling • Fraudulent contact details updation • Fraudulent Account opening • Monitoring for frequent changes in KYC details / account opening details • Mule accounts
Employees	Listening to dealer calls (voice surveillance)	• Unauthorized trading • Password Sharing

		Email surveillance, Surprise visit of dealing rooms Access to trading floor should be access controlled and subject to approvals by designated approvers IP analysis to track internal IPs for self-trading client Restriction on mobile and smart watch or any other device capable of communication both incoming and outgoing in dealing room.	• Front running • Insider Trading • Fraud • Data misuse

	Internet access policies to restrict social networking sites on office network except for legitimate official purposes and to protect data upload on third party websites. Verification of trade with pre-approval, periodic training of employees. Code of Conduct for Dealers / Front running Policy Reporting of misconduct/frauds employee to senior management/committee Unpublished Price Sensitive Information (UPSI) restricted to relevant employees only Access control mechanism by giving access to client data on a need-to know basis Background screening checks at the time of hiring	
	Whistle blower policy to report any fraudulent activity	• Internal fraud or wrongdoing
	Monitoring email sent outside organization for senior employees	• Data protection or any wrongdoing
Authorised Persons	Surprise visit at Authorised Person's office posing as a client Social media monitoring to check if Authorised Persons are misusing Trading Members's logo or promising any assured return 'Authorised Person' level pattern of trading, deviations from normal pattern Recorded call verification on sample basis Scrip level analysis of 'Authorised Person' to check if the 'Authorised Person' is concentrating in any particular Scrip 'Authorised Person' screening against negative databases Calls to clients mapped to 'Authorised Person's on sample basis	• Unauthorized trading • Fraudulent trading activity • Offering assured returns • Unauthorized use of terminal • Opening mule accounts
CEO / MD	Whistle blower policy to report any fraudulent activity.	Internal or Market Fraud or Wrong Doing
KMPs	Monitoring email sent outside organisation for senior employees	Data protection or any wrong doing
Promoters	Whistle blower policy to report any fraudulent activity.	Internal or Market Fraud or Wrong Doing

Monitoring and reporting:

For effective monitoring, we have framed a surveillance policy covering :

Receipt and review of Alerts from Exchanges / generated at our end as mentioned above. Our observations and the reason / rationale for such transactions would be recorded and also submitted to the Exchanges And Depositories as per the set guideline times.

A register is maintained to register all the alerts generated.

All the transactional alerts provided by Depositories and Exchanges are monitored and reviewed – the status shall be No deviations Observed, Verified & Closed, Verified & Reported to the Exchanges / Depositories including action taken at a period not exceeding 30 days.

With respect to alerts generated at our end, we shall report adverse observations along with details of action to Depositories, Exchanges And FIU IND, at a period not later than one week from observing the alerts. In case of any delay in disposition of the alerts beyond the stipulated period, the reason for the same shall be documented.

Suspicious / Manipulative activity will be identified from the above alerts and if we do not receive or not satisfied with the Explanation received or if it is found to be abnormal in nature, the Principal Officer will review the same and after apprising it to the Designated Director or independently as the situation demands, confidentially reports to the FIU IND, Depositories, Exchanges, SEBI or any other regulatory as deemed fit and take appropriate action including that of suspending the Client and with holding the Funds / Securities.

Such Record will be maintained for a period of Five years or such period as may be prescribed by the regulators from time to time or as required till the completion of the inquiry.

Obligation of Reporting of status of the Alerts Generated internally and by the Exchange/Depositories:

To Exchanges/Depositories:
The duly approved status of the alerts to be notified to the Exchanges/Depositories/FIU/ other regulators, as per the time line fixed by such regulators from time to time. The review of such alerts generated shall be notified on Quarterly basis within 15 days from the end of the Quarter to the Exchanges and Depositaries.

Status of Alerts generated Reporting format the Depository / Exchange

Type of Alert	No. of alerts pending at the beginning of quarter	No. of new alerts generated in the quarter	No. of alerts Verified & closed in the quarter	No. of alerts pending at the End of the Quarter	No. of exception cases observed

Any major surveillance action taken during the quarter shall also be reported.

Sr. No.	Brief action taken during the quarter

Such reporting to be made to the Regulators as per the provisions provided by the Regulators through

Electronic upload / mail / physical as desired by the regulators. **Nil** reporting also needs to be uploaded.

To the Board of Directors:
A detailed MIS report along with the count of Alerts generated, its status and the reason for pendency shall be placed before the Board on **Quarterly basis**, It reviews the adequacy and efficiency of the systems for internal control and reporting, analysing the relevant data and any exception noticed during the disposition of alerts and initiates appropriate action where ever necessary and approves the same.

Accountability matrix:

Accountability grid for different types of suspicious behavior:

Surveillance Alerts relating to	**Responsibility of trade surveillance on**
CEO/Executive Director(s)/Senior Management / KMP/Promoters	Board of Directors/Audit Committee
Employees	Compliance Team/Senior Management /Principal Officer/ Designated Director
Clients	Heads of the Department under the guidance of Compliance Team/Senior Management /Principal Officer/ Designated Director.
Authorised Persons	Heads of the Department under the guidance of Compliance Team/Senior Management /Principal Officer/ Designated Director.

Obligation of Principal/Compliance Officer/Designated Director/ Internal / Concurrent Auditor :

i.) The surveillance process and activities shall be conducted under the overall supervision of the Compliance Officer in co ordination with the Principal Officer/ Designated Director.

ii.) The Designated Director shall be responsible for all surveillance activities and shall put up the MIS before the Board on Quarterly Basis, on the number of alerts pending at the beginning of the quarter, generated during the quarter, disposed off during the quarter and pending at the end of the quarter. Reasons for pendency shall be discussed and appropriate action taken. Also, the Board shall be apprised of any exceptions noticed during the disposition of alerts.

iii.) The Internal auditor shall review the surveillance policy, its implementation, effectiveness and review the alerts generated during the period of audit and shall record the observations with respect to the same in their report. Internal Auditor shall verify that the quarterly MIS Report is prepared and placed before the Board.

Conflict of Interest:

In order to maintain utmost confidentiality and avoid tipping of information on all the Alerts generated and Reported on the surveillance activates, As per the policy we have identified the surveillance department as critical and no other person other than the authorized surveillance team shall have physical access to all the records, information and activities. **Chinese Wall** policies and procedures are adopted to prevent

unauthorized exchange of information between critical and non-critical departments.

Whistle Blower Policy:

We have formulated the Whistle Blower Policy to instill confidence in the securities market by prevention and detection of fraud or market abuse, to raise concerns about suspected fraudulent, unfair or unethical practices, violations of regulatory or legal requirements or governance vulnerability.

We have established a Whistle Blower Committee under the supervision of our Principal Officer Mr. Lakshmikanth Inani and the Designated Director,Mr. Vishnukanth Inani, who shall be acting as Whistle Blower Redressal Head and shall be responsible for reviewing the complaints and working under the guidance and instruction of Whistle Blower Committee.

In accordance with the policy, the Committee has formulated a mechanism to raise concerns or complaints under this Policy. This policy applies to all employees, Authorised persons their employees, vendors, shareholders and clients and Directors of the Company.

As per the policy any person can register / raise concern/ complaint on Dedicated email Id wb_surv@inanisec.in or by post to Redressal Head, Inani Securities Limited, G-15 Raghav Ratna Towers Chirag Ali Lane Abids Hyderabad- 500001

We have established procedures to ensure the confidentiality and adequate protection on the anonymity of the identity of the whistle blowers. Ensuring normal treatment and shall not be subjected to any adverse employment action such as demotion, suspension, threats, harassment, or discrimination.

The Whistle Blower Committee shall meet within 15 working days of receiving a complaint under these regulations and shall take appropriate steps as per the Policy.

The Whistle-Blower Redressal Head will conduct an initial review of the complaint and report the findings to the Whistle Blower Committee. The Committee shall base on the genuineness may have detailed Investigation In case of complaints against the Board of Directors, key managerial persons, CEOs, Managing Directors or Promoters, it shall be addressed to the Audit Committee and any complaint is against an employee, it shall be addressed to the Compliance Officer. The Compliance Officer will ensure that the policy is implemented in accordance with SEBI guidelines.

Any False complaints with malicious intent will be viewed seriously and are subject to Disciplinary Action as per the management's decision.

This Whistle Blower policy shall be reviewed and approved annually by the Board to ensure its effectiveness or whenever there is any amendment or change in the regulations.

Fulfillment of Surveillance Obligation:

All the Surveillance Obligations to be fulfilled in true spirit, which includes processing, monitoring and timely reporting of the status of alerts generated at Regulatory end and our end. Any such delay may attract disciplinary action by the management and the regulators.

Review:

This policy shall be reviewed as and when there are any changes introduced by any statutory authority or as and when it is found necessary to change the policy due to business needs but not exceeding period of one year

This policy is monitored and reviewed by the principal officer, Designated Director and Internal Auditor.

Approval Authority:

This Policy was placed before the board and was reviewed in its Board meeting held on **30/06/2025** And was approved by the Board of Directors.