FAIR INTERMEDIATE INVESTMENT PVT. LTD.

CDSL
Your Depository
ISO 27001 Certified

OUTSOURCING POLICY & PROCEDURES
FOR BROKING AND DEPOSITARY PARTICIPANT OPERATIONS

Dated 05.11.2025

This updated policy draft by Fair Intermediate Investments Private Limited (FIIPL) incorporates the latest SEBI Master Circulars for Stock Brokers (August 2024/June 2025) and Depositories (December 2024), while also retaining the core principles of the original 2011 Guidelines.

Regulatory Reference: SEBI Master Circular for Stock Brokers (SEBI/HO/MIRSD/MIRSD-PoD/P/CIR/2025/90) and SEBI Master Circular for Depositories (SEBI/HO/MRD/MRD-PoD-1/P/CIR/2024/168).

1. Applicability

Fair Intermediate Investments Private Limited (FIIPL), as a SEBI-registered stock/commodity broker and Depository Participant (DP-CDSL), will conduct due diligence and ensure high service standards. This policy governs the use of third-party service providers ("Outsourcers") to perform activities related to the services offered by FIIPL.
As per these guidelines, Outsourcing means the use of one or more than one third party ["outsourcer(s)"] - either within or outside the group - by a registered intermediary to perform the activities associated with services which the intermediary offers. In other terms, outsourcing involves transferring responsibility for carrying out an activity of an intermediary (previously carried on internally) to an outsourcer for an agreed charge. The outsourcer provides services to the customer (intermediary) based on a mutually agreed service level, normally defined as per mutual terms and conditions or as per a formal contract.

Many commercial benefits have been ascribed to outsourcing, the most common amongst these being:

- Reducing the organization's costs.
- Greater focus on core business by outsourcing non-core functions.
- Access to world-class skills and resources.

Accordingly, the Company announces this Outsourcing policy.

1. Objective:

This comprehensive policy is being announced and implemented to provide guidance to the Board (i.e. Board of Directors of the **Company**) in assessing whether and how the outsourced activity(ies) may be outsourced. The objective of this policy is to specify, inter alia, (i) the scope of the policy (ii) the criteria for selection of an outsourcing company. outsourcer (iii) nature of activities to be outsourced (iv), various controls to reduce the risks associated with outsourcing and (v) to ensure the high standards of services all the time as well as proper care in the Company's operations.

3. Activities Prohibited from Outsourcing (Core Functions)

In alignment with updated SEBI mandates, FIIPL shall not outsource its core business activities or compliance functions.

- **Stock Broking Core Activities:** Execution of client orders and monitoring of trading activities.
- **Depository Participant Core Activities:** Dematerialization of securities and maintenance/safekeeping of Beneficial Owner (BO) data.
- **Compliance:** Internal audit coordination and regulatory reporting to SEBI/Exchanges.
- **KYC Requirements:** While certain support activities may be assisted by technology, FIIPL remains responsible for compliance with SEBI {KYC Registration Agency} Regulations.

4. Selection and Due Diligence of Outsourcers

Before entering an agreement, FIIPL must conduct and document rigorous due diligence on the provider's:

- **Financial Soundness:** Ability to sustain service levels.
- **Reputation:** Market feedback and past performance record.
- **Infrastructure:** Compatibility of IT systems and security protocols.
- **Disaster Recovery:** Existence of robust Business Continuity Plans (BCP) and Cyber Resilience frameworks.

5. Mandatory Contractual Obligations

All outsourcing relationships must be governed by a legally binding written contract including:

- **Right to Audit:** Unrestricted access for FIIPL, SEBI, and relevant Exchanges to the outsourcer's records and premises.
- **Confidentiality:** Strict non-disclosure of proprietary and customer data, persisting even after contract termination.
- **Sub-contracting:** Prohibition of further outsourcing by the vendor without FIIPL's prior written consent.
- **Termination:** Clear exit strategies to ensure service continuity during transition.

6. Monitoring and Reporting

- **Suspicious Transactions:** FIIPL remains responsible for reporting any suspicious activities identified via outsourced processes to the Financial Intelligence Unit (FIU).

- **Annual Review:** The Board shall review the outsourcing policy and existing arrangements annually to ensure they remain fit for purpose in the changing business environment.
- **Cyber Security:** Regular reporting of any AI/ML applications or systems used by the outsourcer as per the 2024/2025 Master Circular requirements.

The executives Directors & CEO shall be jointly authorized to approve the outsourcing activity in compliance with SEBI's captioned circular dated December 15, 2011.

7. Review of Policy and Assessing Outsourcing Risks

The outsourced activities will be reviewed by the Executive Directors and CEO of the Company at regular intervals, as they consider appropriate in view of the changing business environment.
Apart from regular review and monitoring of the outsourcing policy, the Executive Directors and CEO will have the overall responsibility to ensure that all outsourcing decisions taken by the Company and activities carried out by third parties are in conformity with the outsourcing policy.
Further, the Executive Directors and CEO will be responsible for assessing and evaluating risks during the review of outsourcing activities and take necessary action if any anomalies are found during the process. Risks associated with outsourcing can be classified as operational risk, reputation risk, legal risk, country risk, exit-strategy risk, counter party risk, etc. The Board of Directors of the Company will review the outsourcing activities once in a financial year.

8. Risk Management Programmed:

a. Evaluation of Third Party

As a part of comprehensive outsourcing risk management programme, the executives Directors & CEO shall assess the materiality of the outsourced activity based on the factors as follows: The impact of failure of third party to adequately perform the activity, on the financial, reputational and operational performance of the Company and on the investors / clients; Ability of the Company to cope up with the work, in case of non performance or failure by third party by having suitable back-up arrangements; Regulatory status of third party including its fitness and probity status; Situations involving conflict of interest between the Company and the third party and the measures put in place by the Company to address such potential conflicts, etc.

The risk assessment shall be done prior to signing / renewing the outsourcing contract.

b. Outsourcing to Related Party

In case the Company is desirous of appointing any group entity/ associate of the Company as the third party for outsourcing of activities, it shall take due care and ensure that an arm's length distance has been maintained between the Companies and subject to compliance of the Companies Act 2013 and SEBI's captioned circular dated December 15, 2011.

c. Maintenance of Records

The records relating to all activities outsourced shall be preserved centrally i.e. at the registered office so that the same is readily accessible for review by the Board and/ or other concern department or regulators as and when needed. The Directors & CEO shall ensure that such records are regularly updated and may also form part of the corporate governance review by the management.

- ## Accountability of the Company:

- The Company shall be fully liable and accountable for the activities that are being outsourced to the same extent as if the service were provided in-house.
- Outsourcing arrangements shall not affect the rights of an investor or client against the Company in any manner. The Company shall be liable to the investors for the loss incurred by them due to the failure of the third party and also be responsible for redressal of the grievances received from investors arising out of activities rendered by the third party.
- The facilities / premises / data that are involved in carrying out the outsourced activity by the third party shall be deemed to be those of the Company and that the Company itself and Regulator or the person's authorlzed by it shall have the right to access the same at any point of time.
- Outsourcing arrangements shall not impair the ability of SEBI/SRO or auditors to exercise its regulatory responsibilities such as supervision / inspection of the Company.

- ## Due Diligence and Monitoring of the Third Party:

The Company shall all the time exercise due care, skill, and diligence in the selection of the third party and ensure that the third party has the ability and capacity to undertake the provision of the service effectively.
The due diligence undertaken by the Company shall include assessment of:

- third party's resources and capabilities, including financial soundness, to perform the outsourcing work within the timelines fixed;
- compatibility of the practices and systems of the third party with the intermediary's requirements and objectives;
- market feedback of the prospective third party's business reputation and track record of their services rendered in the past;
- level of concentration of the outsourced arrangements with a single third party; and
- the environment of the state/ country/ region where the third party is located.

- ## Contracts and Agreements:

A formal contract between the Company and the outsourcer shall be entered to protect the interest of both the parties. Proper care shall be taken to ensure that the Outsourcing contract:

a. clearly defines what activities are going to be outsourced, including appropriate service and performance levels;
b. provides for mutual rights, obligations and responsibilities of the Company and the outsourcer, including indemnity;
c. provides for the liability of the outsourcer to the Company for unsatisfactory performance/ other breach of the contract
d. provides for the continuous monitoring and assessment by the Company of the outsourcer so that any necessary corrective measures can be taken up immediately, i.e., the contract shall enable the Company to retain an appropriate level of control over the outsourcing and the right to intervene with appropriate measures to meet legal and regulatory obligations;
e. includes, where necessary, conditions of sub-contracting by the Outsourcer;
f. has unambiguous confidentiality clauses to ensure protection of proprietary and customer data during the tenure of the contract and also after the expiry of the contract;
g. specifies the responsibilities of the outsourcer with respect to the IT security and contingency plans, insurance cover, business continuity and disaster recovery plans, force majeure clause, etc.;
h. provides for preservation of the documents and data by outsourcer;
i. provides for the mechanisms to resolve disputes arising from implementation of the outsourcing contract;
j. provides for termination of the contract, termination rights, transfer of information and exit strategies;
k. neither prevents nor impedes the Company from meeting its respective regulatory obligations, nor the regulator from exercising its regulatory powers; and
l. provides for the Company and /or the regulator or the persons authorized by it to have the ability to inspect, access all books, records and information relevant to the outsourced activity with the outsourcer.

- ### Contingency Plans:

The Company and its outsourcer shall establish and maintain contingency plans, including a plan for disaster recovery and periodic testing of backup facilities. Specific contingency plans shall be separately developed for each outsourcing arrangement, as is done in individual business lines. Further:

a The Company shall take appropriate steps to assess and address the potential consequence of a business disruption or other problems at the Company's level as well as at the outsourcer's level.
b lt shall consider and co-ordinate the contingency plans at both the levels.
c To ensure business continuity, robust information technology security is a necessity. A breakdown in the IT capacity may impair the ability of the Company to fulfill its obligations to other market participants/ clients/ regulators and could undermine the privacy interests of its customers, harm the Company's reputation, and may ultimately impact on its overall operational risk profile. The Company shall, therefore, seek to ensure that the outsourcer maintains appropriate IT security and robust disaster recovery capabilities.
d Periodic tests of the critical security procedures and systems and review of the backup facilities shall be undertaken by the Company to confirm the adequacy of the outsourcer's systems.

- ## Confidentiality:

The Company shall take appropriate steps to require that the outsourcer protects confidential information of both the Company and its customers from intentional or inadvertent disclosure to unauthorized persons. The Company shall take proper care to:

a protect its proprietary and confidential customer information and ensure that it is not misused or misappropriated.
b ensure that the employees of the outsourcer have limited access to the data handled and only on a "need to know" basis and the outsourcer shall have adequate checks and balances to ensure the same.
c ln cases where the outsourcer is providing similar services to multiple entities, the Company shall ensure that adequate care is taken by the outsourcer to build safeguards for data security and confidentiality.
d ln instances, where the Outsourcer acts as an outsourcing agent for multiple intermediaries, the Company shall take proper care and ensure that strong safeguards are put in place so that there is no co-mingling of information / documents, records and assets.

Disclaimer:

This Outsourcing Policy is prepared by the Company in terms of SEBI's Circular No. CIR/MIRSD/24/2011 dated 15th December, 2011 for internal circulation only. The use of this Policy or any matter contained herein, in any manner, without the express written permission from the Company may lead to legal proceedings against the user at the sole discretion of the Company.

Policy created by: Kuldeep Trivedi
Policy reviewed by: Mansi Nagrath
Policy reviewed on: 05th Nov 2025
Policy approved by: Board of Directors Policy approved on: 05th Nov 2025