Allvest Securities Private Limited

POLICY ON OUTSOURCING ACTIVITIES

Document Revision and Version Control

Version No.	Month	Prepared by	Reviewed By	Adopted in Board
Ver 1	Feb-26	Bhoumik Mehta	Amit Bansal	23-02-2026

CONTENTS

INTRODUCTION/ BACKGROUND

Allvest Securities Private Limited (hereinafter referred to as "ASPL" or "Company") is incorporated under the Companies Act, 2013, with Corporate Identification Number (CIN) U66120MH2025PTC440678. ASPL is registered as Stock Broker with SEBI having Registration number INZ000330839 and is registered as Trading Cum Self Clearing Member with National Stock Exchange of India Ltd and NSE Clearing Ltd. (Member Code: 90469), as a Trading Member with BSE Ltd. (Member Code:6973), as a Trading Cum Self Clearing Member with Multi Commodity Exchange of India Limited (Member Code :57650) and ASPL is also registered with SEBI as a Depository Participant having Registration No.: IN-DP-837-2026 and with NSDL having DP ID: IN304949.

PURPOSE

This Outsourcing Policy establishes a framework for ASPL to outsource specific activities to third-party service providers. The policy aims to ensure effective risk management, regulatory compliance, and protection of client interests, thereby maintaining the integrity of operation.

Objectives of the Policy:

- **Operational Efficiency:** Facilitate the outsourcing of non-core activities to enhance efficiency, reduce operational costs, and enable a focus on core competencies.
- **Risk Management:** Ensure that risks associated with outsourcing are systematically identified, assessed, and effectively mitigated.
- **Regulatory Compliance:** Comply with the guidelines issued by SEBI and stock exchanges regarding outsourcing, aiming to protect client interests and uphold accountability.
- **Data Security and Confidentiality:** Safeguard sensitive client data and maintain confidentiality during the outsourcing of functions.

SCOPE OF POLICY

In compliance with the SEBI vide Circular CIR/MIRSD/24/2011 dated December 15, 2011 issued Guidelines on Outsourcing of Activities by Intermediaries ("SEBI Circular"). This policy applies to all functions that are outsourced by ASPL, whether within or outside India, including but not limited to:

- IT services and infrastructure management
- Data storage, processing, and management
- Call centers and customer support

- Legal and accounting services
- Market research and analysis
- Any other activity not considered a core business function that is deemed necessary for outsourcing

CORE BUSINESS ACTIVITIES

Certain core functions that are critical to ASPL's operations, client interests, or direct regulatory obligations shall not be outsourced, including but not limited to:

- Execution of client orders.
- Monitoring of trading activities of clients.
- Dematerialization of securities.
- Investment-related activities.
- Regulatory compliance and reporting.
- Financial control and decision-making.
- Key functionaries mandated to the organization.
- Client grievance redressal.
- Risk management and surveillance functions.

GOVERNANCE FRAMWORK

The Board of ASPL or Committee of the Board of the ASPL to which powers have been delegated shall be responsible inter alia for the following: approval of the framework to evaluate the risks and materiality of all existing and prospective outsourcing and the policies that apply to such arrangements; laying down appropriate authorities for outsourcing depending on risks and materiality; setting up a suitable administrative framework of senior management for the purpose of these directions; undertaking regular reviews of outsourcing strategies and arrangements for their continued relevance and safety and soundness; and deciding on business activities of a material nature to be outsourced and approving of such arrangements.

The Senior Management of the ASPL shall evaluate the risks and materiality of all existing and prospective outsourcing, based on the framework approved by the Board; developing and implementing sound and prudent outsourcing policies and procedures commensurate with the nature, scope, and complexity of the outsourcing activity; reviewing periodically the effectiveness of policies and procedures; communicating information pertaining to material outsourcing risks to the Board in a timely manner;

ensuring that contingency plans, based on realistic and probable disruptive scenarios, are in place and tested; ensuring that there is independent review and audit for compliance with set policies; and undertaking periodic reviews of outsourcing arrangements to identify new material outsourcing risks as they arise.

Policy Coverage: This policy covers activities or the nature of activities that can be outsourced, the authorities who can approve the outsourcing of such activities, and the selection criteria for third parties to whom the activities can be outsourced. For example, an activity shall not be outsourced if it would impair the supervisory authority's right to assess or its ability to supervise the business of ASPL. The risks associated with outsourcing may be operational risk, reputational risk, legal risk, country risk, strategic risk, exit-strategy risk, counter party risk, concentration and systemic risk. The policy is based on an evaluation of risk concentrations, limits on the acceptable overall level of outsourced activities, risks arising from outsourcing multiple activities to the same entity, etc.

RISK MANAGEMENT PROGRAMME

ASPL shall establish a comprehensive outsourcing risk management programme to address outsourced activities and relationships with third-party service providers.

ASPL shall assess outsourcing risk based on several factors, including the scope and materiality of the outsourced activity. Factors to consider in the risk management programme include:

- The impact of a third party's failure to adequately perform the activity on the financial, reputational, and operational performance of ASPL, as well as on investors/clients.
- The ability of ASPL to manage work in case of non-performance or failure by a third party, through suitable backup arrangements.
- The regulatory status of the third party, including its fitness and probity status.
- Situations involving conflicts of interest between ASPL and the third party, and measures put in place to address such potential conflicts.

OUTSOURCING ACTIVITIES TO GROUP COMPANY(IES)

ASPL is committed to adhering to the SEBI guidelines on outsourcing certain activities to group companies or associates. The following principles will be strictly observed:

- **Arm's Length Relationship**: When outsourcing activities to a group entity or associate, ASPL shall maintain an arm's length distance between itself and the third party. This includes separation in terms of infrastructure, manpower, decision-making, record-keeping, and other operational aspects to avoid any potential conflict of interest.

- **Risk Management Practices**: The risk management framework applied to outsourcing arrangements with group entities or associates shall be identical to the practices adopted when outsourcing to unrelated third parties.
- **Disclosures in Contractual Agreements**: All necessary disclosures regarding the relationship between ASPL and the group entity or associate shall be explicitly included as part of the contractual agreement governing the outsourcing arrangement.

Records of all outsourced activities must be stored centrally for easy access by the Board and senior management. These records should be regularly updated and may be included in ASPL's corporate governance review.

The Board of ASPL shall mandate regular reviews of the outsourcing policies, risk management systems, and regulatory requirements by internal or external auditors, as deemed necessary. Additionally, ASPL shall conduct periodic assessments of the financial and operational capabilities of the third party to ensure its continued ability to fulfill its outsourcing obligations.

COMPLIANCE FOR OUTSOURCING ARRANGEMENTS

ASPL shall ensure that outsourcing arrangements neither diminish its ability to fulfill obligations to customers and regulators, nor impede effective supervision by the regulators. The following aspects must be considered before engaging in outsourcing activities:

- ASPL shall be fully liable and accountable for the activities that are outsourced, to the same extent as if the services were provided in-house.
- Outsourcing arrangements shall not impact an investor's or client's rights against ASPL. ASPL remains liable for losses caused by third-party failures and is responsible for addressing grievances related to the third party's activities.
- The facilities, premises, and data used by the service provider for outsourced activities are considered to belong to ASPL. ASPL, along with the regulator or authorized individuals, has the right to access these facilities, premises, and data at any time.
- Outsourcing arrangements shall not hinder SEBI, SRO, or auditors from fulfilling their regulatory duties, including the supervision and inspection of ASPL.

DUE DILIGENCE IN SELECTION OF THIRD PARTY

ASPL shall conduct appropriate due diligence in selecting third parties and in monitoring their performance. It is imperative that ASPL exercises due care, skill, and

diligence in the selection of third parties to ensure they have the ability and capacity to effectively undertake the provision of the service.

ASPL's due diligence shall include an assessment of:

- The third party's resources, capabilities, and financial stability to meet outsourcing deadlines.
- The alignment of the third party's practices and systems with ASPL's goals.
- Market feedback on the third party's reputation and past service track record.
- The concentration of outsourced work with a single third party.
- The operating environment of the foreign country where the third party is based.

COMPLIANCE FOR OUTSOURCING CONTRACTS

ASPL shall ensure that outsourcing relationships are governed by written contracts that clearly outline all key aspects of the arrangement, including the rights, responsibilities, and expectations of both parties, client confidentiality, termination procedures, and other relevant terms.

Outsourcing arrangements shall be governed by a clear, legally binding written contract between ASPL and each third party. The contract's nature and detail shall be appropriate to the significance of the outsourced activity in relation to ASPL's ongoing business.

Care shall be taken to ensure that the outsourcing contract:

- Clearly defines the activities to be outsourced, including appropriate service and performance levels.
- Specifies mutual rights, obligations, and responsibilities of ASPL and the third party, including indemnity clauses.
- Outlines the third party's liability to ASPL for unsatisfactory performance or breaches of the contract.
- Enables ASPL to continuously monitor and assess the third party, allowing immediate corrective measures to ensure control and meet legal and regulatory obligations.
- Includes conditions for sub-contracting by the third party, ensuring ASPL maintains control over risks when outsourcing further.
- Contains unambiguous confidentiality clauses to protect proprietary and customer data during and after the contract period.
- Specifies the third party's responsibilities regarding IT security, contingency plans, insurance, business continuity, disaster recovery plans, and force majeure clauses.
- Requires the third party to preserve documents and data.
- Provides mechanisms for resolving disputes arising from the outsourcing arrangement.

- Details the contract's termination rights, transfer of information, and exit strategies.
- Addresses country-specific risks and obstacles when outsourcing to foreign third parties, including choice-of-law provisions, covenants, and jurisdiction clauses for dispute resolution.
- Ensures the contract does not hinder ASPL's regulatory obligations or the regulator's powers.
  Grants ASPL, the regulator, or authorized persons access to inspect and review all relevant records and information regarding the outsourced activity.

CONTINGENCY PLANS AND DISASTER RECOVERY

ASPL and its third parties 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.

ASPL shall take appropriate steps to assess and address the potential consequences of business disruptions or issues at the third-party level. This includes:

- Considering contingency plans at the third party.
- Coordinating contingency plans between ASPL and the third party.
- Implementing contingency plans at ASPL in the event of non-performance by the third party.

To ensure business continuity, robust information technology security is essential. A breakdown in IT capacity may:

- Impair ASPL's ability to fulfill its obligations to market participants, clients, and regulators.
- Undermine customer privacy.
- Harm ASPL's reputation.
- Impact its overall operational risk profile.

Therefore, ASPL shall ensure that third parties maintain appropriate IT security and robust disaster recovery capabilities.

Periodic tests of the critical security procedures and systems and review of the back- up facilities shall be undertaken by ASPL to confirm the adequacy of the third party's systems.

PROTECTION OF CONFIDENTIAL INFORMATION

ASPL shall take appropriate steps to ensure that third parties protect confidential information of both its own and its customers from intentional or inadvertent disclosure to unauthorized persons.

ASPL is committed to taking appropriate steps to protect its proprietary and confidential customer information and ensure it is not misused or misappropriated.

ASPL shall require third parties to ensure that their employees have limited access to the data handled and only on a “need to know” basis. Third parties must have adequate checks and balances in place to ensure this.

In cases where third parties provide similar services to multiple entities, ASPL shall ensure that adequate care is taken by the third parties to build safeguards for data security and confidentiality.

MANAGING CONCENTRATED OUTSOURCED ACTIVITIES

ASPL recognizes the potential risks when outsourced activities of multiple intermediaries are concentrated with a limited number of third parties. In such cases, both the third party and ASPL must ensure strong safeguards to prevent the co-mingling of information, documents, records, and assets.

ASPL shall ensure that third parties implement robust measures to:

- Segregate information, documents, and records for different intermediaries.
- Maintain distinct storage and access controls to protect the confidentiality and integrity of each intermediary's data.

COMPLIANCE FOR DATA SECURITY

ASPL is committed to ensuring the highest levels of data protection for its operations and client information. All third-party service providers, employees, and key officials must adhere to the following measures:

- All sensitive data, particularly client data, must be encrypted during transmission and storage.
- Only authorized personnel with a legitimate business need should have access to sensitive data at the outsourced entity level. Access logs must be maintained and regularly reviewed.
- ASPL’s data must be segregated from that of other clients of the service provider to prevent data contamination or unauthorized access.
- Service providers are required to maintain data for the period stipulated by ASPL, after which it must be securely deleted.
- Service providers shall maintain the minimum data necessary for providing services and for regulatory purposes only.

- In the event of a data breach or security incident, service providers are obligated to notify ASPL within 24 hours, outlining the nature of the breach, remedial actions, and impact assessment

EMPLOYEE AND KEY OFFICIAL OBLIGATIONS

Employees and key officials who are involved in outsourcing arrangements or handle sensitive data are bound by the following responsibilities:

- Data Handling: Employees must ensure that data shared with service providers is strictly limited to what is necessary for the outsourced activity. They must exercise due caution in sharing sensitive information.
- Regulatory Compliance: Employees and officials must comply with all relevant regulations and ensure that outsourced services meet ASPL's legal obligations.
- Internal Monitoring: Employees assigned to monitor outsourcing arrangements must regularly assess the performance of service providers, including the effectiveness of data protection controls and other regulatory requirements, including IT and Cybersecurity.
- Reporting and Escalation: Any risks or issues identified in relation to outsourced services must be promptly reported to the concerned official (senior management, if required) and escalated for immediate corrective action.

REPORTING TO FINANCIAL INTELLIGENCE UNIT - INDIA

ASPL shall be responsible for reporting of any suspicious transactions / reports to FIU or any other competent authority in respect of activities carried out by the third parties.

VENDOR OBLIGATIONS

All third-party service providers ("Vendor or Service Provider) shall be bound by the following minimum obligations:

- Data Security: Vendors must implement stringent data protection measures to safeguard client and company data from unauthorized access, loss, or misuse. Data access must be limited on a "need-to-know" basis.

- Confidentiality: Vendors must agree to maintain confidentiality of all client and company information and not disclose it to any third party unless authorized by the Company or required by law.

- Compliance with Laws: Vendors must comply with all applicable laws, regulations, and guidelines, including those related to SEBI and other regulatory provisions, data protection, privacy, and information security.

- Right to Audit: The Company reserves the right to audit the vendor's processes, systems, and controls to ensure compliance with contractual obligations and regulatory requirements.
- Annual Reports: Vendors must provide an annual audited report on their financial and operational performance, including an assessment of their internal controls over data security and other regulatory requirements.
- Subcontracting Restrictions: Vendors shall not further subcontract any outsourced activities without prior written approval from the Company.

VENDOR SELECTION AND DUE DILIGENCE

Before entering into any outsourcing arrangement, ASPL shall conduct comprehensive due diligence on the prospective service provider. The due diligence process shall assess:

- The financial strength, resources, capabilities, and market reputation of the service provider, including financial soundness to perform the outsourcing work within the fixed timelines.
- Compatibility of the practices and systems of the service provider with ASPL requirements and objectives.
- Market feedback on the prospective service provider's business reputation and track record of services rendered in the past.
- The provider's ability to meet the ASPL service level requirements.
- The level of concentration of the outsourced arrangements with a single service provider.
- The provider's IT infrastructure, business continuity, and disaster recovery capabilities, including a Business Continuity and Disaster Recovery Plan in place to ensure uninterrupted service to ASPL and for taking care of contingencies.
- The provider's compliance with applicable regulatory frameworks.
- Potential conflicts of interest and concentration risk.
- The provider's commitment to data security and confidentiality.
- Compliance with the cybersecurity and other IT infrastructure and control requirements.
- Ability to provide the products and services required.
- Financial stability of the vendor.
- Vendor reputation in the industry.

- Vendor compliance with applicable laws and regulations.
- Vendor commitment to protecting ASPL's confidential information.
- Physical presence of the vendor in India / outside India.
- Comparative analysis of techno-commercial aspects of the proposal/s received from the vendor.
- Technical competency, compatibility with present setup, support and maintenance, quality and security certifications by the vendor.
- Cost of the product/services.

Before engaging with a vendor or third-party service provider, ASPL will conduct due diligence & proper screening, which will include:

- Conducting reference checks.
- Physical verification of security controls whenever required.
- Risk assessment to determine the security risk, to be carried out before making changes to the provision of services as per the risk management process.

REPORTING AND DISCLOSURE BY SERVICE PROVIDER

Service Providers are required to provide regular reports to ASPL, including:

- **Service Performance Reports:** A periodical report outlining the performance of outsourced activities against service level agreements.
- **Incident Reports:** Immediate reporting of any service interruptions, security breaches or regulatory non-compliance.
- **Annual Audited Reports:** A periodic report detailing the service provider's financial health, IT security controls and risk management practices must be provided to the Company.
- **Performance Monitoring of Vendors and Service Providers:** ASPL shall regularly monitor the performance of vendors and third-party service providers to ensure that they meet ASPL expectations and comply with contractual obligations. This may include conducting periodic reviews, site visits, VAPT and audits.
- **Continuous Monitoring of Cloud Service Providers:** For cloud service providers, continuous monitoring shall be carried out by ASPL to review the technical, legal and regulatory compliance of the provider and take corrective measures / ensure the vendor takes corrective measures wherever necessary.

Financial Stability and Security Risk Assessment of Vendors: ASPL will also monitor the financial stability of vendors to ensure that they remain viable partners. All Service

Provider contract renewals or changes would require security risk assessment to be carried out. This will also include the criticality of business systems and processes involved.

In case of termination, the following should be ensured:

- Service Provider access to ASPL information systems is disabled.
- Confidential information with the Service Provider, as well as subcontractors, is returned / destroyed as per the terms of agreement.
- Service Provider shall be mandated to provide training to new vendors in coming to ensure smooth transition

Relevant data should be backed up and shared with ASPL as well as purged at vendor's end.

TRAINING AND AWARENESS

ASPL may provide awareness to employees involved in vendor management to ensure that they understand the requirements of this policy and the importance of selecting and managing vendors and third-party service providers in accordance with best practices. Information exchange between vendor and ASPL should be through secure communication channels.

REVIEW OF POLICY AND UPDATES

This policy will be reviewed and updated as required to incorporate any changes introduced by regulatory authorities. Additionally, it will undergo periodic reviews at least once in a year to ensure continued relevance, effectiveness, and alignment with current regulatory requirements and industry standards.