PP Capital
Your Profit. Our Aim.

PAWAN PARMESHWAR CAPITAL PVT LTD

Regd. Office: 187, Dadiseth Agyari Lane, 4th Floor, Singhania Wadi, Mumbai – 400 002
Head Office: 136-138, ORM Wing B Co-Op Premises Soc. Ltd., Ground Floor, Royal Palm, Goregaon East, Mumbai – 400 065
Tel: 022-22014936 / 4961 3718

Member: NSE Code: 00188 | BSE Code: 0550

Outsourcing Policy

Version 2.0

Policy Title	Outsourcing Policy
Version	2.0
Date of Approval	16th Oct 2025
Effective Date	20th Oct 2025
Owner	Compliance Department
Approving Authority	Board of Directors of Pawan Parmeshwar Capital Pvt Ltd
Next Review Date	Annually, or earlier upon regulatory change or material outsourcing event
Replaces	Outsourcing Policy (legacy version, in force prior to this revision)

1. Introduction and Purpose

Pawan Parmeshwar Capital Pvt Ltd ("the Company") is a Stock Broker registered with the Securities and Exchange Board of India ("SEBI") and is a Trading Member of the National Stock Exchange of India Ltd (NSE Code 00188) and BSE Limited (BSE Code 0550). In the course of conducting its business, the Company may from time to time outsource certain activities to third-party service providers.

This Outsourcing Policy is framed to govern the outsourcing arrangements entered into by the Company in compliance with SEBI Circular CIR/MIRSD/24/2011 dated December 15, 2011 on "Guidelines on Outsourcing of Activities by Intermediaries" (the "Outsourcing Circular"), the SEBI Master Circular for Stock Brokers dated June 17, 2025, the SEBI (Stock Brokers) Regulations, 1992 (as amended), and applicable bye-laws, rules and regulations of the Stock Exchanges and Clearing Corporations.

The policy aims to ensure that outsourcing arrangements do not compromise the Company's regulatory obligations, the interests of its clients, the integrity of the securities markets, or the Company's ability to discharge its responsibilities to SEBI, the Stock Exchanges and other regulatory authorities.

2. Scope and Applicability

This policy applies to:

- All outsourcing arrangements entered into by the Company, whether with related parties, group entities, or unrelated third parties.
- Outsourcing arrangements covering activities ancillary to the Company's core stock broking business such as information technology services, data centre and cloud hosting, network services, back-office operations support, data entry and digitisation, document management, courier and printing, facility management, recordkeeping, and similar support services.
- Both new outsourcing arrangements and ongoing arrangements that pre-date this policy, with the latter to be brought within the policy framework within a reasonable transition period.

This policy applies to all departments, the Compliance Officer, the Risk Management function, the Information Technology function, and all members of the Board of Directors of the Company.

3. Definitions

For the purposes of this policy:

4. Regulatory Framework

This policy is framed with reference to and in compliance with, inter alia, the following:

- SEBI Circular CIR/MIRSD/24/2011 dated December 15, 2011 on Guidelines on Outsourcing of Activities by Intermediaries (the "Outsourcing Circular").

- SEBI (Stock Brokers) Regulations, 1992 (as amended from time to time, including Chapter IVA inserted by SEBI (Stock Brokers) (Amendment) Regulations, 2024 notified on June 27, 2024).
- SEBI Master Circular for Stock Brokers SEBI/HO/MIRSD/MIRSD-PoD/P/CIR/2025/90 dated June 17, 2025.
- SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/96 dated July 4, 2024 on responsibilities of stock brokers.
- SEBI Cybersecurity and Cyber Resilience Framework for SEBI Regulated Entities dated August 20, 2024 (as clarified on April 30, 2025) ("CSCRF").
- Digital Personal Data Protection Act, 2023 and rules made or to be made thereunder.
- Information Technology Act, 2000 and rules made thereunder.
- Bye-laws, Rules, Regulations and Circulars of the Stock Exchanges (NSE, BSE) and Clearing Corporations (NSE Clearing Limited, Indian Clearing Corporation Limited) as applicable from time to time.
- SEBI (Prohibition of Insider Trading) Regulations, 2015 and the Company's Insider Trading Code v2.0 in respect of confidentiality of Unpublished Price Sensitive Information.

5. Activities That Shall NOT Be Outsourced (Core Activities)

In accordance with Paragraph 5.2 of the Outsourcing Circular, the Company shall not outsource its core business activities and compliance functions. The following functions are identified as core and shall be performed in-house by the Company:

- Know Your Client (KYC) functions including verification of identity, documentation and final acceptance of the client.
- Order management decisions, dealing and execution functions on the trading terminals of the Stock Exchanges.
- Risk management functions including pre-trade and post-trade risk controls, margin assessment, and position monitoring.
- Compliance functions including regulatory reporting, dealing with regulators, the Stock Exchanges and Clearing Corporations, and the office of the Compliance Officer.
- Internal audit functions, except in the manner permitted by SEBI to engage external firms to conduct internal audit while retaining responsibility internally.
- Investment decisions and discretionary management of client assets.

- Activities requiring SEBI registration in their own right (e.g., research analyst functions, investment advisory functions) which shall not be outsourced to an unregistered entity.
- Handling of client funds and client securities, except such ancillary operational support (such as banking and DP services from regulated entities) as the regulatory framework expressly contemplates.
- The principal-officer and key managerial responsibilities including those of the Principal Officer under the Prevention of Money Laundering Act, 2002.

This list is illustrative and not exhaustive. Where any doubt exists as to whether an activity falls within the prohibited core category, the matter shall be referred to the Compliance Officer for a determination, which shall be placed before the Board for ratification.

6. Activities That MAY Be Outsourced

Subject to compliance with this policy, the Outsourcing Circular and the regulatory framework, the Company may outsource certain ancillary activities including:

- Information technology infrastructure services including data centre hosting, server administration, cloud computing services, network management and connectivity services.
- Software development, application maintenance and software support services.
- Back-office operations support such as data entry, reconciliation support, and digitisation of records.
- Recordkeeping, archival, document storage and document management services.
- Printing, courier, dispatch and bulk mailing services.
- Facility management, security services, housekeeping, and physical asset management.
- Call centre and customer support handling for non-discretionary, scripted client communication (subject to compliance with the Mobile Phone Usage Policy and recording requirements).
- Specialised professional services such as legal, tax, accounting (subject to engagement of qualified professionals), and consulting advisory.
- Training and human resource support services.
- Engagement of external firms to conduct internal audit, half-yearly internal audit of operations, system audit and information security audit (subject to applicable regulatory requirements regarding qualification of such auditors and the Company retaining ultimate responsibility).

All such outsourcing arrangements shall be subject to the due diligence, contractual, monitoring and oversight requirements set out in this policy.

7. Principles Governing Outsourcing

The Company shall ensure that all outsourcing arrangements adhere to the following overarching principles set out in the Outsourcing Circular:

7.1 Accountability and Responsibility

The Board of Directors and the senior management of the Company shall retain ultimate responsibility for all outsourced activities. Outsourcing shall not diminish the Company's obligations to its clients, to SEBI, the Stock Exchanges and the Clearing Corporations, or to any other regulator.

7.2 No Dilution of Regulatory Obligations

Outsourcing of any activity shall not result in any dilution of the Company's responsibility for compliance with applicable laws, regulations, circulars, bye-laws and rules. The Company shall remain answerable to its clients and regulators in respect of all outsourced activities as if such activities were performed by the Company itself.

7.3 Confidentiality of Client and UPSI Information

The confidentiality of client information, including personal data within the meaning of the DPDP Act, 2023, and the confidentiality of Unpublished Price Sensitive Information within the meaning of the SEBI (Prohibition of Insider Trading) Regulations, 2015 shall be preserved at all times. The Service Provider shall be bound by contractual non-disclosure and confidentiality obligations no less stringent than those binding on the Company itself.

7.4 No Conflict of Interest

The Service Provider shall not be a related party or affiliate whose engagement would compromise the independence of the activity outsourced. Where a Group Entity is engaged as Service Provider, the conflict of interest provisions of the Company's Conflicts of Interest Policy v2.1 shall apply.

7.5 Proportionality

The extent of due diligence, contractual provisions and ongoing oversight shall be commensurate with the materiality of the outsourcing arrangement, the sensitivity of the activity and the risk profile of the Service Provider.

8. Pre-Outsourcing Due Diligence

Before entering into any outsourcing arrangement, the Company shall conduct due diligence on the proposed Service Provider, covering at a minimum the following parameters:

- Identity, ownership structure and legal status of the Service Provider, including verification of registered office, registration with applicable authorities, and details of the controlling persons or beneficial owners.
- Financial soundness of the Service Provider, evidenced by the most recent audited financial statements, where available.
- Technical capability and human resources of the Service Provider to deliver the proposed services to the required standards.
- Operational experience and track record, including reference checks with existing clients of the Service Provider, where feasible.
- Reputation in the industry, including review of any adverse media reports, regulatory actions, litigation history and similar matters.
- Information security controls, business continuity arrangements, disaster recovery capabilities and cybersecurity posture of the Service Provider, particularly for IT-related outsourcing.
- Compliance posture of the Service Provider with applicable laws including the DPDP Act, 2023, the Information Technology Act, 2000, and tax registrations.
- Existence and adequacy of insurance cover maintained by the Service Provider.
- Conflict of interest assessment, particularly where the Service Provider is a Group Entity or has dealings with clients or competitors of the Company.

The due diligence shall be documented and a Vendor Due Diligence Checklist substantially in the form set out in Annexure A shall be completed and signed off by the proposing department head and the Compliance Officer before the outsourcing arrangement is approved.

For Material Outsourcing arrangements, the due diligence report shall additionally be placed before the Board of Directors for review prior to engagement.

9. Outsourcing Agreement: Mandatory Contractual Provisions

Every outsourcing arrangement shall be governed by a written agreement executed between the Company and the Service Provider. The agreement shall, at a minimum, contain provisions covering:

- Scope of services to be provided, with clear and detailed description of the activities, deliverables, service levels and operational metrics.

- Performance standards including service level agreements (SLAs), turnaround times, uptime commitments (for IT services), and remedial actions in the event of non-performance.
- Fees, billing arrangements, payment terms, and the basis for any variable consideration.
- Duration of the arrangement, renewal terms, and notice periods for termination.
- Confidentiality and non-disclosure obligations binding the Service Provider and all its personnel handling Company data or client data, surviving the termination of the agreement, and aligned with the DPDP Act, 2023.
- Data protection, data security, data residency (preference for data hosted within India), data segregation from other clients of the Service Provider, and data return or destruction on termination.
- Information security standards to be maintained by the Service Provider, including access controls, encryption requirements, audit logging, incident reporting timelines, and alignment with the CSCRF (where applicable to the Company).
- Business continuity and disaster recovery obligations of the Service Provider, including recovery time objectives (RTO) and recovery point objectives (RPO) commensurate with the criticality of the activity.
- Right of the Company, its internal auditors, its statutory auditors, SEBI, the Stock Exchanges and the Clearing Corporations to inspect the books, records, infrastructure and personnel of the Service Provider in relation to the outsourced activity, on demand and without prior notice if so required by the regulator.
- Right of the Company to demand reports, certifications and audit results from the Service Provider, including third-party assurance reports where available.
- Indemnification by the Service Provider for losses arising from the Service Provider's acts, omissions, breach of contract, negligence or fraud.
- Restriction on the Service Provider sub-contracting the outsourced activity without the prior written consent of the Company; and, where sub-contracting is permitted, the Service Provider shall remain primarily responsible to the Company for the acts and omissions of the sub-contractor.
- Termination rights of the Company, including the right to terminate for cause (including breach, regulatory action against the Service Provider, change in control of the Service Provider, and material deterioration in financial condition) and the right to terminate for convenience on reasonable notice.

- Smooth transition assistance and exit management obligations on termination including transfer of data, records and operations to the Company or its nominated successor Service Provider in an orderly manner.
- Governing law (Indian law), jurisdiction (preference for the courts of Mumbai), and dispute resolution mechanism.
- Compliance with all applicable Indian laws including SEBI regulations, the DPDP Act, 2023, the Information Technology Act, 2000, tax laws, and labour laws.

10. Approval Workflow for Outsourcing Arrangements

The approval workflow for outsourcing arrangements shall be as follows:

10.1 Routine Outsourcing

Routine outsourcing arrangements involving non-material services (such as courier, printing, housekeeping, and similar) of value not exceeding Rs. 5,00,000 per annum may be approved by the Head of the relevant Department in consultation with the Compliance Officer, and shall be reported in the Outsourcing Register.

10.2 Significant Outsourcing

Outsourcing arrangements of value exceeding Rs. 5,00,000 but not exceeding Rs. 25,00,000 per annum, or relating to IT services, recordkeeping, or services involving access to client data, shall be approved by the Compliance Officer jointly with the Managing Director or senior management designee, and shall be reported to the Board at the next ensuing meeting.

10.3 Material Outsourcing

Material Outsourcing arrangements, including arrangements of value exceeding Rs. 25,00,000 per annum, all outsourcing of IT infrastructure, data hosting, application support that processes client trading or KYC data, and any outsourcing to a Group Entity, shall be approved by the Board of Directors prior to engagement. The Board approval shall be based on a due diligence report and proposed agreement placed before it.

The monetary thresholds set out above may be revised by the Board from time to time without amendment to this policy. The Compliance Officer shall maintain the up-to-date threshold table in the Outsourcing Register.

11. Ongoing Monitoring and Oversight

The Company shall continuously monitor and oversee the performance of each Service Provider through the following mechanisms:

- Periodic review meetings between the Department Head responsible for the outsourced activity and the Service Provider, at a frequency commensurate with the criticality of the activity but not less than once per quarter for Material Outsourcing.
- Tracking of SLA compliance through monthly or quarterly performance reports submitted by the Service Provider.
- Annual review of all Material Outsourcing arrangements by the Compliance Officer and presentation of findings to the Board of Directors as part of the annual compliance review.
- Periodic review of the Service Provider's continued financial soundness, regulatory standing, and information security posture.
- Monitoring of incidents, complaints, breaches and service disruptions, with documented escalation, root cause analysis and remediation.
- Periodic confirmation from the Service Provider of compliance with contractual obligations, including confidentiality and information security obligations.

The Compliance Officer shall maintain an Outsourcing Register substantially in the form set out in Annexure B, capturing details of every outsourcing arrangement, key contractual terms, review history and incidents.

12. Business Continuity Considerations for Outsourced Activities

The Company shall ensure that outsourcing does not impair its ability to continue operations in the event of disruption to the Service Provider. For every Material Outsourcing arrangement:

- The Service Provider shall maintain documented business continuity and disaster recovery arrangements, and shall share the relevant policy and test results with the Company on request.
- The Company shall maintain a documented contingency plan for the activity outsourced, including identification of an alternate Service Provider or arrangements for bringing the activity back in-house on short notice.
- The Company's overall Business Continuity Plan shall incorporate scenarios involving failure of each Material Service Provider, with defined recovery procedures.
- Joint business continuity testing with the Service Provider shall be conducted at least once per year, where feasible.

Failure of the Service Provider shall not be accepted as an excuse for the Company's failure to discharge its obligations to clients, the Stock Exchanges, Clearing Corporations or SEBI.

13. Confidentiality, Data Privacy and Information Security

The Company recognises that outsourcing arrangements may involve sharing of confidential information including client personal data, financial data, trading data and Unpublished Price Sensitive Information with the Service Provider. Accordingly:

- All Service Providers shall be bound by comprehensive confidentiality and non-disclosure obligations, surviving the termination of the outsourcing agreement.
- Personal data shall be shared with the Service Provider only on a need-to-know basis and only to the extent necessary for performance of the outsourced activity, in compliance with the DPDP Act, 2023 and applicable rules. The Service Provider shall be designated as a Data Processor and the Company shall remain the Data Fiduciary.
- Where the outsourced activity may involve access to UPSI, the Service Provider's personnel handling such information shall be designated as Designated Persons or shall be subject to comparable contractual obligations of confidentiality, and shall be entered in the Structured Digital Database maintained under the Insider Trading Code v2.0.
- Information security controls implemented by the Service Provider shall meet the standards prescribed under the CSCRF (where applicable to the Company) and contractually flow through to the Service Provider.
- The Service Provider shall report all security incidents, data breaches and suspected unauthorised access to the Compliance Officer without delay, and in any event within 24 hours of detection.
- On termination or expiry of the outsourcing agreement, the Service Provider shall return or, at the Company's option, securely destroy all Company data and confidential information in its possession, and shall furnish a written certificate to that effect.

Cross-reference: Conflicts of Interest Policy v2.1, Insider Trading Code v2.0, Mobile Phone Usage Policy v1.0, Risk Management and Surveillance Policy v2.0, Internal Control Policy v2.0.

14. Special Considerations for Cloud and IT Outsourcing

Where IT services, data hosting or application services are outsourced (including cloud computing arrangements):

- Data residency shall be assessed and, to the extent practicable and required by applicable law, data shall be hosted within India.
- The Service Provider shall maintain industry-recognised information security certifications (such as ISO/IEC 27001, SOC 2 Type II) commensurate with the criticality of the data and activity.

- The Service Provider shall implement encryption of data in transit and at rest, role-based access controls, multi-factor authentication for privileged access, comprehensive logging and audit trails, and timely security patching.
- The Service Provider shall provide the Company with access to audit logs and security event records for the Company's environment on request.
- Arrangements shall comply with the SEBI Cybersecurity and Cyber Resilience Framework (CSCRF) dated August 20, 2024 (as clarified on April 30, 2025) to the extent applicable to the Company.
- Sub-contracting by the cloud or IT Service Provider (such as use of underlying infrastructure providers) shall be transparently disclosed and assessed for risk.

15. Outsourcing to Group Entities

Where outsourcing is proposed to a Group Entity:

- The arrangement shall be structured at arm's length on terms that are no less favourable to the Company than would be the case in an unrelated party arrangement.
- All requirements of due diligence, contractual provisions, monitoring and oversight applicable to unrelated Service Providers shall apply equally to the Group Entity.
- The arrangement shall be reviewed and approved by the Board of Directors and shall be assessed against the Conflicts of Interest Policy v2.1.
- The Group Entity shall not be permitted to exercise any control or influence over the Company's regulatory or compliance decisions by virtue of the outsourcing relationship.

16. Restrictions on Outsourcing

Notwithstanding any other provision of this policy, the Company shall not enter into an outsourcing arrangement that:

- Would involve outsourcing of any Core Activity as listed in Section 5.
- Would compromise the Company's ability to discharge its regulatory obligations to SEBI, the Stock Exchanges, the Clearing Corporations or any other authority.
- Would impair the right of SEBI, the Stock Exchanges, the Clearing Corporations or other regulators to inspect or examine the Company or the outsourced activity.
- Would expose client funds or client securities to undue risk.
- Would involve the transfer of confidential client information outside India in contravention of applicable law.

- Is structured in a manner that allows the Service Provider to make decisions reserved for the Board, senior management or Compliance Officer of the Company.

17. Termination and Exit Management

Every outsourcing agreement shall include comprehensive provisions for orderly termination and exit. On termination of an outsourcing arrangement:

- The Service Provider shall transfer all Company data, records, documents and operational files to the Company or to its nominated successor Service Provider in an agreed format and within an agreed timeframe.
- The Service Provider shall continue to perform the outsourced services during the transition period to ensure no disruption to the Company's operations and its services to clients.
- The Service Provider shall return or destroy, at the Company's option, all confidential information and personal data in its possession, and shall furnish a written certificate to that effect.
- The Compliance Officer shall conduct a post-termination review to ensure that all obligations have been discharged and that there is no residual risk to the Company or its clients.
- The termination, transition and any incidents arising therefrom shall be recorded in the Outsourcing Register.

18. Reporting, Records and Governance

18.1 Reporting to the Board

The Compliance Officer shall present to the Board of Directors:

- All proposed Material Outsourcing arrangements, prior to engagement, with the due diligence report and proposed agreement.
- A quarterly summary of all outsourcing arrangements entered into, modified or terminated during the quarter.
- An annual review of all subsisting outsourcing arrangements, performance against SLAs, incidents and remedial actions.
- Any incident of significant service failure, data breach, regulatory action against a Service Provider, or material concern relating to a Service Provider, as soon as practicable after becoming aware.

18.2 Records

The Company shall maintain the following records in respect of outsourcing arrangements:

- Outsourcing Register substantially in the form of Annexure B, capturing details of all outsourcing arrangements current and historical.
- Vendor Due Diligence Checklists for each Service Provider engaged, signed off by the Compliance Officer.
- Copies of executed outsourcing agreements together with all amendments and renewals.
- Periodic performance reports, audit reports and incident reports received from Service Providers.
- Board approvals, sub-committee approvals and senior management approvals for outsourcing arrangements.
- Termination notices, exit management records and post-termination certifications.

All records shall be retained for not less than 8 (eight) years from the date of termination of the outsourcing arrangement, or such longer period as may be prescribed by applicable law or as may be required by reason of pending proceedings.

19. Roles and Responsibilities

Responsibility for compliance with this policy is allocated as follows:

- Board of Directors: Approves the policy and any subsequent amendments; approves Material Outsourcing arrangements; reviews annual reporting on outsourcing; takes ultimate responsibility for all outsourced activities.
- Managing Director / Senior Management: Approves Significant Outsourcing arrangements jointly with the Compliance Officer; supervises implementation; escalates material concerns to the Board.
- Compliance Officer (Mr. Rajkumar Pandey): Owns and maintains this policy; reviews and signs off on all due diligence; maintains the Outsourcing Register; coordinates with Service Providers on confidentiality, regulatory inspections and reporting; presents periodic reports to the Board.
- Department Heads: Identify outsourcing needs within their functions; conduct day-to-day monitoring of Service Providers under their oversight; ensure performance against SLAs; report incidents to the Compliance Officer.
- Information Technology Function: Conducts technical due diligence on IT-related Service Providers; oversees ongoing information security compliance by IT Service Providers; coordinates joint business continuity testing.

- All employees: Comply with confidentiality obligations in respect of any Service Provider with whom they interact; report any concerns about Service Provider conduct or service failures to the Compliance Officer or their reporting manager.

20. Policy Review and Amendments

This policy shall be reviewed annually by the Compliance Officer and any proposed amendments shall be placed before the Board of Directors for approval. The policy shall also be reviewed and updated in response to:

- Any amendment to the Outsourcing Circular, the SEBI (Stock Brokers) Regulations, the Master Circular for Stock Brokers, the DPDP Act, 2023 (and rules thereunder), the CSCRF or other applicable legal or regulatory framework.
- Material changes in the Company's business model, scale of operations, or extent of outsourcing.
- Significant outsourcing incidents that suggest a need for policy strengthening.
- Observations from SEBI or Stock Exchange inspections, internal audit, or external assurance reviews.

Annexure A — Vendor Due Diligence Checklist (Template)

To be completed by the proposing Department Head and signed off by the Compliance Officer before engagement of any Service Provider.

Field	Details / Evidence
Name of Proposed Service Provider	
Registered Office and Principal Place of Business	
Legal Constitution (Co/LLP/Partnership/Prop.)	
PAN / GSTIN / CIN	
Principal Contact Person and Designation	
Scope of Services Proposed	
Proposed Term and Annual Fees	
Is this a Material Outsourcing? (Y/N — with reasons)	
Is this a Group Entity? (Y/N)	
Audited Financial Statements Reviewed (last year)	
Reference Checks Conducted (list of references)	
Industry Reputation and Adverse Media Check	
Regulatory / Legal Proceedings Disclosed	
Information Security Posture (certifications, controls)	
Business Continuity and Disaster Recovery Arrangements	

Data Residency (within India? Y/N)	
Insurance Cover Maintained	
DPDP Act and Confidentiality Provisions in Agreement	
SEBI / Exchange Inspection Rights in Agreement	
Termination and Exit Management Provisions	
Conflict of Interest Assessment	
Recommendation of Department Head	
Compliance Officer Sign-Off (Name, Date, Signature)	
Approval Authority (Dept Head / MD+CO / Board)	
Date of Approval	

Annexure B — Outsourcing Register (Template)

To be maintained by the Compliance Officer. Format may be implemented in electronic or physical form.

Field	Particulars
Serial Number	
Name of Service Provider	
Scope of Outsourced Activity	
Material Outsourcing? (Y/N)	
Group Entity? (Y/N)	
Date of Agreement Execution	
Term of Agreement	
Annual Contract Value	
Department Head Responsible	
Approval Authority and Date	
Date of Last Due Diligence Review	
Date of Last Performance Review	
Incidents during Review Period	
Renewal / Termination Date	
Remarks	

Board Approval

This Outsourcing Policy (2.0) has been reviewed and approved by the Board of Directors of Pawan Parmeshwar Capital Pvt Ltd at its meeting held on 16-10-2025.

The Board has also recorded, on the same date, the following:

- The Board notes that this policy supersedes any prior outsourcing policy of the Company and aligns the Company with the SEBI Outsourcing Circular dated December 15, 2011, the SEBI Master Circular for Stock Brokers dated June 17, 2025, the DPDP Act, 2023, and the CSCRF dated August 20, 2024 (as clarified on April 30, 2025).
- The Board confirms Mr. Rajkumar Pandey as the policy owner and Compliance Officer responsible for implementation, maintenance of the Outsourcing Register, and quarterly reporting.
- The Board ratifies the monetary approval thresholds set out in Section 10 (Routine: up to Rs. 5,00,000 p.a.; Significant: Rs. 5,00,000 to Rs. 25,00,000 p.a.; Material: above Rs. 25,00,000 p.a., or any IT/data hosting/Group Entity arrangement) and authorises the Compliance Officer to update these thresholds in the Register subject to ratification at the next Board meeting.
- The Board directs management to bring all subsisting outsourcing arrangements within the framework of this policy within 90 days of the Effective Date.
- Cross-references to other policies (Conflicts of Interest Policy v2.1, Insider Trading Code v2.0, Mobile Phone Usage Policy v1.0, Risk Management and Surveillance Policy v2.0, Internal Control Policy v2.0) are noted and the Board confirms that this policy is to be read consistently with such other policies.

For PAWAN PARMESHWAR CAPITAL PVT. LTD.

Director / Authorised Signatory

PAWAN PARMESHWAR CAPITAL PVT. LTD. MUMBAI

Director / Authorised Signatory

Name: Pawankumar Choudhary

Designation: Director

Date: 16-10-2025

Place: Mumbai