

OUTSOURCING POLICY

Savantika Vanijya Pvt Ltd

1. INTRODUCTION:

This policy shall be termed as the Outsourcing Policy for Savantika Vanijya Pvt Ltd (hereinafter referred to as the “Company”). The terms in this policy shall be considered as defined by the Reserve Bank of India (RBI) in Master Direction – Reserve Bank of India (Non-Banking Financial Company - Scale Based Regulation) Directions, 2023 dated 19th October 2023. With the rapid growth in the financial services industry, Non-Banking Financial Companies (NBFCs) have increasingly outsourced various activities to third-party service providers or affiliated entities within a group. Outsourcing allows the Company to focus on core functions while leveraging external expertise for non-core activities. However, outsourcing also exposes the Company to various risks, including strategic, reputational, compliance, operational, legal, and systemic risks.

To mitigate these risks and ensure compliance with regulatory requirements, the Company has formulated this Outsourcing Policy, which is aligned with the RBI’s guidelines on “Managing Risks and Code of Conduct in Outsourcing of Financial Services by NBFCs.

This policy was approved and reviewed by the Board of Directors of the Company on **29th December 2025** and shall be reviewed and amended periodically as required.

2. OBJECTIVE OF THE POLICY:

The objectives of this Outsourcing Policy are to:

- a) Establish a robust governance framework for outsourcing decisions, ensuring Board and senior management oversight
- b) Define clear criteria for identifying activities suitable for outsourcing
- c) Establish standards for the selection, due diligence, and assessment of service providers
- d) Ensure that outsourcing arrangements do not compromise the NBFC's ability to fulfill regulatory obligations
- e) Implement risk management practices commensurate with the risk profile of outsourced activities
- f) Maintain operational resilience through effective business continuity and disaster recovery planning
- g) Ensure compliance with all applicable RBI guidelines, regulatory requirements, and legal obligations

- h) Protect customer interests and confidentiality
- i) Preserve the NBFC's operational independence and ability to supervise and control outsourced functions
- j) Provide mechanisms for regular monitoring, audit, and oversight of service providers

3. SCOPE

This policy covers all outsourcing arrangements, which may be applied including:

- Financial outsourcing (loan sourcing, processing, credit assessment, recovery)
- IT and technology services outsourcing
- Operational and back-office outsourcing
- Third-party sourcing and lead generation
- Vendor management and procurement services
- Compliance and audit-related outsourcing (excluding core compliance functions)
- Custodial and agency services

4. DEFINITION OF OUTSOURCING AND MATERIALITY

4.1 Materiality Threshold

Material outsourcing is defined as any outsourcing arrangement where the service provider's failure or performance issues would, if they occurred, cause a significant impact on the NBFC's:

- Business operations and continuity
- Financial stability, earnings, and profitability
- Liquidity and solvency position
- Risk profile and credit rating
- Regulatory compliance and reputation
- Customer service delivery and protection
- Systemic stability

4.2 Materiality Assessment Criteria

Materiality shall be assessed using the following parameters:

Criteria	Assessment Approach
Business Criticality	Essential vs. Non-essential functions; impact on operations if disrupted
Financial Significance	Cost as % of operating expenses; potential financial loss if service fails
Customer Impact	Impact on customer service, protection, and grievance resolution
Risk Profile	Strategic, reputational, compliance, operational, and legal risks
Operational Complexity	Complexity and integration with core business processes
Service Provider Concentration	Dependency on single vendor; concentration risk
Regulatory Impact	Impact on regulatory compliance and RBI supervisory access
Time to Recovery	Duration and difficulty of recovery if service is disrupted

4.3 Material vs. Non-Material Outsourcing

Material Outsourcing requires:

- Board approval (before arrangement commencement)
- Comprehensive service level agreements
- Detailed risk assessment
- Regular monitoring and reporting
- Annual Board review
- Enhanced controls and governance

Non-Material Outsourcing requires:

- Senior management approval (within delegated authority)
- Standard service agreements
- Basic risk assessment
- Regular operational monitoring

5. ACTIVITIES THAT CAN BE OUTSOURCED:

The NBFC may outsource the following activities, subject to compliance with RBI guidelines and proper risk management:

5.1 Core Business Activities (Non-Core Functions)

- **Loan Sourcing and Lead Generation:** DSA/DMA-based loan sourcing, online lead generation, and borrower identification (ensuring customer consent and transparency)

- **Loan Documentation and Processing:** Application form collection, document verification, and preliminary processing
- **Credit Assessment Support:** Data compilation and preliminary credit analysis (final approval remains with NBFC)
- **Loan Disbursement and Collection:** Fund transfers, collection of loan installments, and reconciliation
- **Recovery and Follow-up:** Post-default recovery, legal recovery processes, and asset resolution
- **Technology and IT Services:** System maintenance, software development, IT infrastructure management, network operations, cybersecurity services, data center operations
- **Back-Office and Administrative Services:** Data entry and processing, record management, filing, and document archival
- **Customer Support Services:** Query handling, complaint registration, status updates (not core compliance functions)

5.2 Support Services

- **Courier and Logistics Services:** Document courier, physical asset logistics
- **Housekeeping and Facility Management:** Office cleaning, maintenance, security
- **Recruitment and Training:** HR support, recruitment process outsourcing, training delivery
- **Background Verification:** Candidate background checks, employee verification
- **Legal Services:** Contract review, documentation support, compliance monitoring
- **Statutory Compliance Services:** Filing, compliance calendar management (subject to internal verification)
- **Insurance and Asset Protection Services:** Valuations, inspections, insured asset management

5.3 Specialized Services

- **Digital Lending Platform Services:** Loan origination through digital channels, platform management, borrower acquisition
- **Payment Gateway and Settlement Services:** Transaction processing, settlement operations
- **Data Analytics Services:** Non-strategic reporting, trend analysis
- **Marketing and Communications:** Promotional material development, customer communication (not policy communication)

5.4 Outsourcing Principles

All outsourcing decisions must be based on:

- Comprehensive business case and cost-benefit analysis
- Risk assessment and mitigation capability
- Service provider suitability and financial strength
- Availability of appropriate monitoring mechanisms

- Compliance with regulatory requirements

The above list is indicative and not exhaustive. The Company may outsource other activities permissible under RBI guidelines.

6. ACTIVITIES THAT SHALL NOT BE OUTSOURCED:

The following core management functions **must NOT be outsourced** as they are fundamental to NBFC operations and regulatory compliance:

6.1 Strategic Decision-Making Functions

- Board-level strategic planning and policy formulation
- Determination of business strategy and direction
- Capital allocation and budgeting decisions
- Executive compensation and succession planning
- Material risk policy formulation

6.2 Core Compliance Functions

- **Regulatory Compliance Function:** Monitoring and ensuring ongoing compliance with RBI regulations and guidelines
- **KYC Compliance:** Final determination of KYC adequacy and customer acceptance decisions
- **AML/CFT Compliance:** Final assessment of suspicious transactions, STR filing, and AML policy compliance
- **CIC Coordination:** Customer Information Compilation and submission to credit bureaus
- **Fair Practices Code:** Establishment and monitoring of fair lending practices
- **Grievance Redressal:** Final grievance review and resolution mechanism
- **Regulatory Reporting:** Final review and submission of regulatory reports and filings to RBI

6.3 Credit Approval and Control Functions

- **Loan Sanctioning Decisions:** Final approval authority for loan applications and credit decisions
- **Loan Agreement Finalization:** Final review and execution of loan agreements
- **Credit Policy Framework:** Development and approval of credit policies and standards
- **Collateral Valuation:** Final valuation and acceptance of securities (may support with outsourced valuers)
- **Pricing Decisions:** Rate-setting and pricing approval for loan products

6.4 Audit and Control Functions

- **Internal Audit Function:** Core internal audit activities, compliance audits, and regulatory audit coordination (may hire contract auditors subject to Board approval)

- **Risk Management Function:** Formulation and oversight of enterprise risk management
- **Internal Controls:** Design and evaluation of internal control systems and processes
- **Fraud Detection and Investigation:** Final fraud investigation and reporting

6.5 Senior Management Functions

- Board secretariat functions
- Chief Executive Officer functions
- Chief Compliance Officer / Chief Risk Officer functions
- Chief Financial Officer / Finance Head functions (financial statement certification)
- Internal Audit Head functions

6.6 Information and Data Protection Functions

- Final decisions on customer data access and usage
- Data protection policy formulation and oversight
- Information security governance and cyber risk management
- Final approval of data processing arrangements

Note: Supporting functions within the above can be outsourced (e.g., data processing, documentation support) provided final decision-making remains with the NBFC.

7. MATERIAL OUTSOURCING:

Material outsourcing arrangements are those that, if disrupted, could significantly impact the Company's business operations, reputation, or profitability. Materiality shall be assessed based on:

- The significance of the activity to the Company's operations.
- The potential impact on earnings, solvency, liquidity, and risk profile.
- The cost of outsourcing as a proportion of total operating costs.
- The aggregate exposure to a single service provider.
- The impact on customer service and protection.

8. RISK ASSESSMENT AND MANAGEMENT

8.1 Risk Categories

The NBFC shall assess and manage the following risks associated with outsourcing:

8.1.1 Strategic Risk

Definition: The risk that outsourcing decisions are misaligned with the NBFC's strategic objectives or that service provider actions undermine competitive advantage.

Mitigation Measures:

- Ensure outsourcing aligns with overall business strategy
- Establish strategic objectives for each outsourcing arrangement
- Regular strategy reviews with service provider
- Maintain competitive capability in-house for core competencies

8.1.2 Reputational Risk

Definition: Risk that service provider's poor performance, misconduct, or customer-facing interactions damage the NBFC's reputation and brand value.

Mitigation Measures:

- Establish service quality standards and performance metrics
- Ensure service provider adheres to Fair Practices Code and ethical standards
- Regular customer feedback mechanisms
- Quick escalation and remediation of customer complaints
- Maintain NBFC branding on all customer communications
- Regular audits of customer-facing service quality

8.1.3 Compliance and Regulatory Risk

Definition: Risk that service provider's non-compliance with legal, regulatory, or RBI requirements exposes the NBFC to penalties and regulatory action.

Mitigation Measures:

- Include comprehensive compliance clauses in service agreements
- Regular compliance audits and monitoring
- Ensure service provider follows NBFC's compliance procedures
- Establish compliance reporting mechanisms
- Clear delegation of compliance responsibilities
- Regular training of service provider staff on compliance requirements
- Monitor regulatory communications affecting outsourced activities

8.1.4 Operational Risk

Definition: Risk of loss arising from inadequate or failed internal processes, service provider failures, systems failures, fraud, or external events affecting outsourced services.

Mitigation Measures:

- Detailed performance metrics and monitoring
- Regular operational audits
- Fraud detection and prevention mechanisms

- Business continuity and disaster recovery plans
- Systems redundancy and backup arrangement
- Regular testing of contingency arrangements
- Insurance coverage for critical services
- Service level agreement with penalty provisions

8.1.5 Legal and Contractual Risk

Definition: Risk that service agreement terms are inadequate, unenforceable, or expose the NBFC to unexpected liabilities or legal disputes.

Mitigation Measures:

- Comprehensive legal review of all outsourcing agreements
- Clear terms on liability, indemnification, and termination
- Dispute resolution mechanisms
- Jurisdiction and governing law clarity
- IP protection and confidentiality clauses
- Right to audit and RBI inspection access
- Adequate notice periods for termination
- Escrow arrangements for critical data and code

8.1.6 Counterparty Risk

Definition: Risk that service provider lacks financial stability, adequate capacity, or appropriate underwriting standards, leading to inadequate service delivery or financial failure.

Mitigation Measures:

- Financial stability assessment of service provider
- Periodic review of service provider's financial condition
- Capacity and resource assessment
- Insurance and indemnification requirements
- Contingency funding arrangements
- Right to substitute service provider if financial condition deteriorates
- Audit rights over service provider's operational capabilities

8.1.7 Concentration Risk

Definition: Risk of excessive dependence on a single service provider or group, leading to systemic vulnerabilities if that provider fails.

Mitigation Measures:

- Establish concentration limits per service provider
- Avoid over-reliance on any single vendor for critical services
- Develop backup arrangements or secondary providers

- Regular review of concentration exposure
- Ensure no single vendor loss would materially impact operations
- Diversify among multiple vendors for critical functions

8.1.8 Exit Strategy and Reversibility Risk

Definition: Risk that the NBFC cannot effectively exit or terminate an outsourcing arrangement, or cannot reverse outsourced functions back in-house due to technical, financial, or contractual barriers.

Mitigation Measures:

- Clear exit and transition clauses in agreements
- Service provider obligation to assist with orderly transition
- Data and system ownership clarity
- Escrow arrangements for critical code and data
- Regular testing of exit plans
- Capability to bring critical functions back in-house
- Transition service agreements with defined timeline
- Penalty provisions for poor exit cooperation

8.1.9 Offshore/Jurisdictional Risk

Definition: Risk arising from outsourcing to service providers in foreign jurisdictions, including political, legal, tax, and regulatory uncertainties.

Mitigation Measures:

- Country risk assessment for offshore vendors
- Ensure compliance with all applicable laws in both jurisdictions
- Maintain records and original documents in India
- Ensure RBI's access and inspection rights are preserved
- Data residency requirements - critical customer data retained in India
- Avoid contractual impediments to RBI supervision
- Monitor changes in foreign regulatory environment
- Establish fallback arrangements in case of political/legal disruption

8.1.10 Technology and Cybersecurity Risk

Definition: Risk that service provider's technology systems are inadequate, insecure, or vulnerable to cyber attacks, causing data breaches or service disruptions.

Mitigation Measures:

- Technology assessment and evaluation
- Information security audit of service provider systems
- Cybersecurity standards and requirements in agreements

- Regular security testing and vulnerability assessments
- Incident reporting and response procedures
- Data encryption and access controls
- Regular business continuity and DR testing
- Insurance for cyber risk

9. SELECTION CRITERIA FOR SERVICE PROVIDERS

9.1 Due Diligence Framework

The NBFC shall conduct comprehensive due diligence before engaging any service provider. Due diligence shall cover:

9.1.1 Financial Strength and Stability

- Last 2-3 years of audited financial statements
- Assessment of solvency, liquidity, and profitability
- Credit rating and bank references
- Contingency plans if service provider faces financial stress
- Insurance coverage maintained by service provider
- Exit arrangements if service provider faces financial difficulty

9.1.2 Operational Capabilities and Capacity

- Assessment of technical and operational capabilities
- Review of current clients and service quality track record
- Capacity to handle NBFC's volume and requirements
- Availability of skilled and trained personnel
- Technology infrastructure and systems
- Scalability to accommodate growth
- Compliance with ISO/industry standards
- Quality assurance mechanisms

9.1.3 Regulatory and Compliance Track Record

- Regulatory compliance history and track record
- Past regulatory actions or penalties
- Compliance certifications (ISO 27001 for IT services, etc.)

- Understanding of financial services compliance requirements
- Anti-money laundering and KYC compliance capabilities
- Data protection and privacy compliance

9.1.4 Information Security and Data Protection

- Information security policies and frameworks
- Certification for data protection (ISO 27001, RBI guidelines compliance)
- Cybersecurity measures and incident response procedures
- Business continuity and disaster recovery capabilities
- Data encryption and access control measures
- Regular security audits and penetration testing
- Background verification of employees

9.1.5 Business Continuity and Disaster Recovery

- Business continuity policy and procedures
- Disaster recovery plan with tested mechanisms
- Recovery time objective (RTO) and recovery point objective (RPO)
- Geographic redundancy for critical systems
- Regular testing and updates of DR plans
- Third-party disaster recovery site if applicable
- Insurance coverage for business interruption

9.1.6 Experience and References

- Years of experience in the relevant service area
- Experience in serving financial services sector
- References from existing clients (with permission)
- Case studies of similar outsourcing arrangements
- Track record of service delivery excellence
- Management team qualifications and experience

9.1.7 Conflict of Interest Assessment

- Independence from NBFC ownership and management
- No significant business interests that could create conflicts
- If group company, ensure arm's length basis of arrangement
- No connections to NBFC's competitors or adverse parties

- Clear separation of NBFC's business from other service provider's clients

10. ROLE OF THE BOARD AND SENIOR MANAGEMENT:

10.1. Role of the Board:

- Approve the outsourcing policy and framework for risk evaluation.
- Define delegation of authority based on risks and materiality.
- Review outsourcing strategies and arrangements periodically.

10.2. Responsibilities of Senior Management:

- Evaluate risks and materiality of outsourcing arrangements.
- Develop and implement outsourcing policies and procedures.
- Ensure contingency plans and independent audits are in place.
- Communicate material outsourcing risks to the Board.

11. OUTSOURCING TO GROUP COMPANIES:

The Company may outsource activities to group companies, provided:

- Arm's length distance is maintained in decision-making and resource sharing.
- Written agreements specify the scope of services, charges, and confidentiality clauses.
- Customers are informed about the entity offering the product/service.

12. OFF-SHORE OUTSOURCING:

For off-shore outsourcing, the Company shall:

- Assess and monitor country risks, including political, social, and legal conditions.
- Ensure that original records are maintained in India and that RBI's supervisory access is not hindered.

13. OUTSOURCING AGREEMENTS:

All outsourcing arrangements shall be governed by legally binding written agreements that include:

- Scope of services, performance levels, and confidentiality clauses.
- Rights to access books, records, and information.
- Termination clauses, dispute resolution mechanisms, and exit strategies.
- Provisions for RBI inspection and audit access.

14. CLIENT CONFIDENTIALITY & SECURITY:

The Company shall ensure that service providers:

- Protect customer information and limit access on a “need-to-know” basis.
- Isolate the Company’s data from other clients.
- Report security breaches promptly.

15. RESPONSIBILITIES OF DSAs/DMAs/RECOVERY AGENTS:

- DSAs/DMAs/recovery agents shall adhere to the Company’s Fair Practices Code.
- They shall refrain from intimidation, harassment, or misleading representations.

16. LOANS SOURCED THROUGH DIGITAL LENDING PLATFORMS:

- The Company shall disclose the names of digital lending platforms on its website.
- Sanction letters and loan agreements shall be issued on the Company’s letterhead.
- Oversight and monitoring of digital lending platforms shall be ensured.

17. BUSINESS CONTINUITY AND DISASTER RECOVERY:

- Contingency plans shall be developed for each outsourcing arrangement.
- The Company shall retain control over outsourced activities to ensure business continuity.

18. MONITORING AND CONTROL:

- Regular audits shall assess the adequacy of risk management practices.
- The financial and operational condition of service providers shall be reviewed annually.

19. MAINTENANCE OF RECORDS:

- Records of outsourced activities shall be preserved centrally and updated regularly.
- Half-yearly reviews shall be presented to the Board.

20. GRIEVANCE REDRESSAL:

- A Grievance Redressal Officer shall be appointed to address customer complaints.
- Complaints shall be resolved within 30 days.

21. REPORTING REQUIREMENTS:

The Company shall submit Currency Transaction Reports (CTRs) and Suspicious Transaction Reports (STRs) to the Financial Intelligence Unit (FIU) or other competent authorities.

22. REVIEW OF THE POLICY:

This policy shall be reviewed periodically by the Board of Directors or as and when required.