Document Title: Policy on Outsourcing	Reliance Capital Limited
Originally approved: _____	
Last Reviewed: _____	

Reliance Capital Limited
Policy on Outsourcing

This document is copyright protected in content, presentation, and intellectual origin, except where noted otherwise. You may not modify, remove, augment, add to, publish, transmit, participate in the transfer or sale of, create derivative works from, or in any way exploit any of the elements of this document, in whole or in part without prior written permission from Reliance Capital Ltd. © 2025-2026.

Document Title: Policy on Outsourcing	Reliance Capital Limited
Originally approved: _____	
Last Reviewed: _____	

Table of Contents

1. Introduction
    1.1 Preamble
    1.2 Objectives
    1.3 Applicability
2. Regulatory Framework
3. Definitions
4. Role of the Board and Senior Management
    4.1 Board of Directors
    4.2 Audit Committee (or equivalent)
    4.3 Senior Management / CEO
5. Scope of Outsourcing
    5.1 Activities that can be Outsourced (Illustrative)
    5.2 Activities that cannot be Outsourced
    5.3 Materiality Assessment of Outsourcing Arrangements
6. Outsourcing Process Lifecycle
    6.1 Due Diligence and Vendor Selection
    6.2 Outsourcing Agreement (Service Level Agreement - SLA)
    6.3 Monitoring and Control of Outsourced Activities
    6.4 Review and Performance Assessment
7. Risk Management Framework for Outsourcing
    7.1 Identification and Assessment of Risks
    7.2 Risk Mitigation Strategies
    7.3 Business Continuity and Disaster Recovery
    7.4 Exit Strategy

8. Data Protection, Information Security, and Cybersecurity
9. Grievance Redressal Mechanism
10. Management of Sub-Contracting by Service Providers
11. Cross-Border Outsourcing (If Applicable)
12. Compliance and Regulatory Reporting
13. Internal Controls and Audit
14. Policy Review and Amendment

1. Introduction

1.1 Preamble This Policy on Outsourcing of Financial Services (the "Policy") outlines the robust framework and comprehensive guidelines for all outsourcing activities undertaken by **Reliance Capital Limited (RCL)** (the "Company"). As an unlisted Non-Banking Financial Company - Core Investment Company (NBFC-CIC) registered with the Reserve Bank of India (RBI), the Company recognizes that while outsourcing can enhance efficiency and expertise, it must be managed prudently to avoid transferring inherent risks or diluting its regulatory obligations. This Policy ensures that outsourcing arrangements do not diminish the Company's ability to fulfill its responsibilities to its customers, adhere to regulatory mandates, and maintain the integrity of its operations.

1.2 Objectives The primary objectives of this Policy are to:

- Ensure that all outsourcing arrangements are undertaken in compliance with the latest RBI Master Directions, particularly the **RBI Master Direction – Reserve Bank of India (Outsourcing of Financial Services) Directions, 2023**, and the **Master Direction - Reserve Bank of India (Non-Banking Financial Company - Scale Based Regulation) Directions, 2021**, along with the Companies Act, 2013, and other applicable laws.
- Establish a clear governance structure for oversight and management of outsourcing risks, ensuring that ultimate responsibility for outsourced activities remains with the Company.
- Define a robust framework for identifying, assessing, mitigating, and monitoring all risks associated with outsourcing.
- Prescribe comprehensive due diligence processes for the selection of service providers.

- Ensure that outsourcing agreements clearly define responsibilities, performance standards, data security, and business continuity arrangements.
- Protect customer interests, including privacy, confidentiality, and effective grievance redressal.
- Maintain the Company's ability to operate effectively and meet regulatory expectations, even in the event of a service provider's failure.

1.3 Applicability This Policy applies to all **material outsourcing arrangements** entered into by **RCL** for financial services, whether with an associated entity within the group/conglomerate or with an unrelated third party, located in India or elsewhere. This includes, but is not limited to, outsourcing of IT services, data management and back-office operations. This Policy does not apply to activities that are not related to financial services, such as usage of courier services, catering for staff, housekeeping, janitorial services, security of premises, movement and archiving of records, purchasing of assets, or legal advice.

2. Regulatory Framework

This Policy is formulated and implemented in strict adherence to, but not limited to, the following key regulatory provisions and guidelines issued by the Reserve Bank of India (RBI) and the Ministry of Corporate Affairs:

- **RBI Master Direction – Reserve Bank of India (Outsourcing of Financial Services) Directions, 2023 [DoR.FIN.REC.06/20.10.001/2023-24 dated November 02, 2023] (as amended from time to time):** This is the primary and most comprehensive regulatory directive governing outsourcing for Regulated Entities (REs), including NBFCs.
- **RBI Master Direction – Core Investment Companies (Reserve Bank) Directions, 2016 (as amended from time to time):** Specific provisions applicable to CICs related to their operations and governance.

- **RBI Master Direction – Reserve Bank of India (Non-Banking Financial Company - Scale Based Regulation) Directions, 2021 (as amended from time to time):** This framework categorizes NBFCs and impacts governance, risk management, and IT frameworks, which directly influence outsourcing considerations.
- **RBI Master Direction – Information Technology Framework for the NBFC Sector, 2017 (as amended from time to time):** Provides guidelines on IT governance, information security, IT operations, and cybersecurity.
- **Companies Act, 2013, and relevant rules thereunder:** Especially provisions related to the duties and responsibilities of the Board of Directors, maintenance of records, and general corporate governance principles.
- **IT Act, 2000 and rules thereunder:** Pertaining to data privacy and security.
- Other relevant circulars, notifications, or guidelines issued by the RBI or any other statutory authority.

3. Definitions

For the purpose of this Policy, the following definitions shall apply:

- **Company:** Refers to Reliance Capital Limited.
- **Outsourcing:** The Company's use of a third party (either an intra-group entity or an unrelated entity) to perform activities on a continuing basis that would normally be undertaken by the Company itself, now or in the future. "Continuing basis" includes agreements for a limited period.
- **Financial Services:** Services that directly relate to the Company's core financial activities, such as loan origination support, credit appraisal support, customer interaction services, collections, account servicing, debt management, and IT services integral to financial operations.

- **Material Outsourcing Arrangement:** An outsourcing arrangement which, if disrupted, has the potential to significantly impact the Company's business operations, profitability, reputation, or its ability to manage risk and comply with regulations. The criteria for materiality are further defined in Section 5.3.
- **Service Provider:** A third party (either a group entity or an unrelated entity) that performs outsourced activities for the Company.
- **Board:** The Board of Directors of Reliance Capital Limited.
- **Senior Management:** Refers to the Managing Director/Chief Executive Officer and functional heads of the Company responsible for various operations.
- **Exit Strategy:** A comprehensive plan for orderly termination of an outsourcing arrangement and seamless transition of the outsourced activity, either in-house or to another service provider.
- **Leverage Ratio:** As defined by RBI for CICs, relating to the ratio of outside liabilities to owned funds. Outsourcing should not impact this ratio adversely or circumvent its spirit.

4. Role of the Board and Senior Management

The Board of Directors and Senior Management hold ultimate responsibility for ensuring effective governance and oversight of all outsourcing activities.

4.1 Board of Directors:

- **Overall Responsibility:** The Board holds the ultimate responsibility for outsourced activities and for ensuring that the Company's risk management practices are robust enough to address risks arising from outsourcing.
- **Policy Approval:** Approves the Outsourcing Policy and ensures its periodic review.
- **Material Outsourcing Approval:** Approves all material outsourcing arrangements and significant changes thereto.

- **Risk Appetite:** Defines the Company's risk appetite concerning outsourcing.
- **Oversight:** Periodically reviews the effectiveness of the risk management framework for outsourcing and receives reports from the Audit Committee and Senior Management.
- **Strategic Decisions:** Ensures that outsourcing decisions are part of the Company's strategic planning and not merely a cost-cutting exercise without considering associated risks.

4.2 Audit Committee (or equivalent Board Committee):

- **Review and Oversight:** The Audit Committee (or a similar committee with equivalent responsibilities, if constituted by the Board) shall assist the Board in its oversight function by reviewing the Company's internal controls and risk management processes related to outsourcing.
- **Internal Audit Reports:** Reviews internal audit reports on outsourced activities and ensures that identified deficiencies are promptly addressed.
- **Compliance:** Oversees the Company's compliance with regulatory guidelines on outsourcing.

4.3 Senior Management / CEO:

- **Implementation:** Responsible for the implementation of this Policy and for ensuring that appropriate operational controls are in place for all outsourced activities.
- **Risk Management:** Establishes a sound risk management framework for outsourcing and oversees the identification, assessment, and mitigation of outsourcing risks.
- **Due Diligence:** Ensures that comprehensive due diligence is conducted for all service providers.
- **Contract Management:** Oversees the negotiation and execution of robust outsourcing agreements.

- **Monitoring and Control:** Establishes mechanisms for continuous monitoring and control of outsourced activities.
- **Reporting:** Reports regularly to the Board and/or Audit Committee on the performance and risks of outsourced arrangements.
- **Contingency Planning:** Develops and implements effective business continuity and exit strategies.

5. Scope of Outsourcing

The Company shall clearly define what activities can and cannot be outsourced, with a focus on retaining core competencies and critical functions in-house.

5.1 Activities that can be Outsourced (Illustrative): The following are indicative examples of activities that may be considered for outsourcing, subject to materiality assessment, due diligence, and risk management framework:

- Data processing and management.
- Back-office operations (e.g., account maintenance, reconciliation).
- IT infrastructure management and support.
- Payroll processing.
- Certain aspects of human resources management (e.g., recruitment support).

5.2 Activities that cannot be Outsourced: The following activities are considered core management functions and **shall not be outsourced**:

- Core management functions related to policy formulation, internal audit, compliance, and risk management (including the ultimate responsibility for credit sanction, treasury operations, and internal controls).
- Decision-making on credit applications or other core financial decisions.
- Approval of prudential functions such as capital adequacy and leverage ratio calculations.

- Approval of strategy and policy for investments.
- Any activity that would compromise the RBI's right to supervise or access records, or the Company's ability to maintain oversight.
- Any activity where outsourcing would pose an unacceptable level of operational, reputational, or compliance risk.

5.3 Materiality Assessment of Outsourcing Arrangements: Before entering into any outsourcing arrangement, the Company shall undertake a comprehensive assessment to determine its materiality. An outsourcing arrangement is considered material if:

- It impacts the Company's expected profitability, operations, reputation, or its ability to meet regulatory obligations.
- It involves a significant portion of the Company's operations or assets.
- Its disruption or failure would cause significant financial loss, operational disruption, or reputational damage to the Company.
- It significantly alters the Company's risk profile.

All material outsourcing arrangements require heightened scrutiny, detailed due diligence, Board/IC approval (as per delegation), and rigorous ongoing monitoring.

6. Outsourcing Process Lifecycle

The outsourcing lifecycle shall comprise distinct phases, each with specific requirements to ensure prudent management.

6.1 Due Diligence and Vendor Selection: The Company shall conduct a thorough due diligence process before selecting a service provider, covering:

- **Capability and Reputation:** Assessment of the service provider's expertise, track record, human resources, technological capabilities, and reputation in the market.
- **Financial Health:** Evaluation of the service provider's financial soundness, stability, and capacity to continue providing services.

- **Business Model & Controls:** Understanding the service provider's business model, organizational structure, control environment, and governance practices.
- **Data Protection and Information Security:** Rigorous assessment of the service provider's information security policies, data protection practices, IT infrastructure, cybersecurity framework, and compliance with relevant standards (e.g., ISO 27001). This includes a review of their ability to handle sensitive and confidential customer data securely.
- **Compliance & Legal:** Verification of the service provider's legal and regulatory compliance, including any past adverse regulatory actions or litigations.
- **Business Continuity and Disaster Recovery (BCP/DR):** Evaluation of the service provider's BCP and DR capabilities to ensure resilience and minimize service disruption.
- **Sub-contracting:** Assessment of the service provider's policy on sub-contracting and the due diligence performed on their sub-contractors.

6.2 Outsourcing Agreement (Service Level Agreement - SLA): All material outsourcing arrangements shall be governed by a legally binding written agreement that clearly defines the rights and obligations of both parties. The agreement shall include, but not be limited to, the following clauses:

- **Scope of Services:** Clearly defined services, roles, and responsibilities of both the Company and the service provider.
- **Performance Standards:** Measurable service level agreements (SLAs) with clear performance metrics, targets, and penalties for non-compliance.
- **Confidentiality and Data Security:** Robust clauses on confidentiality of information (especially customer data), data privacy, data ownership, data encryption, access controls, and cybersecurity measures.

- **Right to Audit and Inspect:** The Company's explicit right to audit and inspect the service provider's operations, systems, books, and records related to the outsourced activity, both on-site and remotely. This right extends to the RBI or persons authorized by RBI.
- **Sub-contracting:** Clear conditions and requirements for sub-contracting by the service provider, including the need for the Company's prior written consent and ensuring the original service provider remains responsible.
- **Termination and Exit Strategy:** Comprehensive clauses on termination rights (including for material breach, regulatory non-compliance, or insolvency), notice periods, transition plans, data return/destruction, and responsibilities for a smooth exit.
- **Indemnities:** Indemnification clauses for losses arising from service provider's negligence, breach of contract, or data breaches.
- **Dispute Resolution:** Mechanisms for dispute resolution (e.g., arbitration, mediation) and the governing law/jurisdiction of the agreement (preferably Indian law and jurisdiction).
- **Business Continuity:** Requirement for the service provider to maintain and test BCP/DR plans.
- **Customer Grievance Redressal:** Acknowledgment that the ultimate responsibility for customer grievance redressal remains with the Company.
- **Regulatory Compliance:** Clear statement that the service provider must comply with all applicable regulatory guidelines relevant to the outsourced services and assist the Company in its compliance.

6.3 Monitoring and Control of Outsourced Activities:

- **Designated Owner:** Each outsourced activity shall have a designated business/function owner within the Company responsible for overseeing its performance, risk management, and compliance.
- **Performance Review:** Regular review of the service provider's performance against agreed SLAs and performance metrics.
- **Risk Review:** Continuous monitoring of risks associated with the outsourced activity and the service provider, including financial health, operational issues, and security incidents.
- **Meetings:** Periodic review meetings with service providers to discuss performance, issues, and strategic alignment.
- **Audit Trail:** Maintenance of an adequate audit trail for all outsourced transactions and data movements.

6.4 Review and Performance Assessment:

- **Annual Review:** A comprehensive annual review of all material outsourcing arrangements shall be conducted by the designated owner, assessing performance, compliance, and overall effectiveness.
- **Vendor Rating:** Implementation of a vendor rating mechanism to assess the quality of services and compliance for ongoing relationships.
- **Corrective Actions:** Any deficiencies identified during monitoring or review shall be promptly addressed with the service provider, with clear timelines and accountability for corrective actions.

7. Risk Management Framework for Outsourcing

The Company shall maintain a comprehensive risk management framework specific to outsourcing to identify, assess, mitigate, and monitor all associated risks.

7.1 Identification and Assessment of Risks: The following key risks, among others, shall be identified and assessed for each outsourcing arrangement:

- **Strategic Risk:** Risk of outsourcing not aligning with the Company's strategic goals or weakening its competitive advantage.
- **Reputation Risk:** Risk of adverse public opinion arising from the service provider's actions or failure.
- **Operational Risk:** Risk of disruption to business operations due to service provider failure, technology issues, or inadequate controls.
- **Compliance Risk:** Risk of non-compliance with regulatory requirements or legal obligations due to service provider's actions.
- **Legal Risk:** Risk of lawsuits, penalties, or contractual disputes.
- **Concentration Risk:** Risk arising from over-reliance on a single service provider or a few service providers for critical functions.
- **Systemic Risk:** Risk that failure of a common service provider to multiple REs could have wider systemic implications.
- **Information Security Risk & Cyber Risk:** Risk of data breaches, unauthorized access, or cyber-attacks on the service provider's systems.
- **Country Risk:** For cross-border outsourcing, risks associated with the political, economic, social, and legal environment of the service provider's country.
- **Exit Strategy Risk:** Risk of inability to smoothly transition outsourced activities.

7.2 Risk Mitigation Strategies:

- **Clear Policies & Procedures:** Development of clear internal policies and procedures for outsourcing.
- **Robust Due Diligence:** As detailed in Section 6.1.
- **Strong Contracts:** As detailed in Section 6.2.

- **Internal Controls:** Implementation of strong internal controls and monitoring mechanisms (Section 11).
- **Contingency Planning:** Development of robust BCP and DR plans (Section 7.3).
- **Diversification:** Where feasible, avoiding over-reliance on a single service provider for critical activities.
- **Insurance:** Requiring service providers to maintain adequate insurance coverage.

7.3 Business Continuity and Disaster Recovery (BCP/DR):

- **Service Provider's BCP/DR:** The Company shall ensure that the service provider has sound and tested business continuity and disaster recovery plans that are aligned with the Company's own BCP/DR strategy.
- **Testing:** The Company shall periodically (e.g., annually) review and, where appropriate, participate in the testing of the service provider's BCP/DR plans.
- **Company's Preparedness:** The Company shall have its own contingency plans in place to manage the risk of service provider failure, including the ability to bring outsourced activities in-house or transition to an alternative service provider.

7.4 Exit Strategy:

- A robust exit strategy shall be developed for each material outsourcing arrangement at the outset of the engagement. This strategy shall cover:
    - **Transition Plan:** A clear plan for the orderly termination of the agreement, including data migration, knowledge transfer, and hand-over of processes.
    - **Alternative Arrangements:** Identification of alternative service providers or the capacity to bring the activity in-house.
    - **Data Return/Destruction:** Clear procedures for the secure return or certified destruction of all Company data held by the service provider upon termination.
    - **Cost Assessment:** Assessment of potential costs associated with an exit.

- The exit strategy shall be regularly reviewed and, if feasible, tested.

8. Data Protection, Information Security, and Cybersecurity

The Company is ultimately responsible for the confidentiality, integrity, and availability of its data, including customer data, regardless of where it is stored or processed.

- **Ultimate Responsibility:** The Company retains ultimate responsibility for data protection and information security.
- **Policy Adherence:** Service providers must adhere to the Company's IT and Cybersecurity Policies and Frameworks, as well as all applicable data protection laws and regulations (e.g., IT Act, 2000, and upcoming Data Protection Bill).
- **Security Measures:** The outsourcing agreement must stipulate stringent security measures, including encryption, access controls, network security, incident response plans, and regular security audits.
- **Customer Data Protection:** Special emphasis shall be placed on the protection of personal and sensitive customer data. Data localization requirements (if any) must be strictly adhered to.
- **Breach Reporting:** The service provider shall be contractually obligated to report any security incidents, data breaches, or unauthorized access to the Company immediately. The Company, in turn, will report to the RBI as required.
- **Audit Rights:** The Company, and auditors appointed by it or the RBI, shall have the right to audit the service provider's information systems and processes for security compliance.

9. Grievance Redressal Mechanism

The Company shall ensure that a robust and effective grievance redressal mechanism is in place to address customer complaints arising from outsourced activities.

- **Ultimate Responsibility:** The ultimate responsibility for redressing customer grievances rests with Reliance Capital Limited.
- **Accessibility:** Customers shall have direct access to the Company's grievance redressal channels, even if the service is outsourced.
- **SLA Provisions:** The outsourcing agreement shall clearly specify the service provider's role and responsibilities in the grievance redressal process, including timelines for response and escalation procedures.
- **Training:** Service provider employees involved in customer interaction must be trained on the Company's customer service standards and grievance redressal procedures.
- **Monitoring:** The Company shall monitor customer complaints related to outsourced activities to identify systemic issues and ensure timely resolution.

10. Management of Sub-Contracting by Service Providers

The Company shall exercise strict control over any sub-contracting by its service providers.

- **Prior Approval:** The service provider shall be expressly prohibited from sub-contracting any significant part of the outsourced activity without the Company's prior written consent.
- **Due Diligence on Sub-Contractors:** If sub-contracting is approved, the original service provider shall be responsible for conducting due diligence on the sub-contractor, equivalent to that performed by the Company on the original service provider. The Company retains the right to review this due diligence.
- **Ultimate Responsibility:** The original service provider remains fully responsible to the Company for the outsourced activity, even if sub-contracted.
- **Contractual Flow-down:** The original outsourcing agreement shall stipulate that all terms and conditions relevant to the outsourced activity (e.g., confidentiality, data

security, audit rights, regulatory compliance) must be flowed down to the sub-contractor.

11. Cross-Border Outsourcing (If Applicable)

If the Company engages in cross-border outsourcing (i.e., where the service provider is located outside India), additional considerations and safeguards shall apply:

- **Legal and Regulatory Environment:** Thorough understanding and continuous monitoring of the legal, regulatory, political, and economic environment in the service provider's country, particularly concerning data privacy, bankruptcy laws, and ease of enforcing contracts.
- **Data Localization:** Compliance with any RBI or Indian government regulations regarding data localization, ensuring that critical data is stored and processed within India as required.
- **Access for RBI:** Ensure that the RBI and the Company's auditors retain the right to inspect and audit the service provider's operations, even if located overseas. The agreement must clearly state that the overseas regulator will not obstruct such access.
- **Governing Law:** The outsourcing agreement for cross-border arrangements shall preferably be governed by Indian law, with Indian courts having jurisdiction, to the extent legally feasible.
- **Systemic Implications:** Assessment of any systemic implications if the foreign service provider serves multiple REs.

12. Compliance and Regulatory Reporting

The Company is responsible for ensuring continuous compliance with all regulatory requirements related to outsourcing.

- **Compliance Department Role:** The Compliance Department shall periodically review outsourcing arrangements to ensure adherence to this Policy and relevant RBI guidelines.
- **Reporting to RBI:** The Company shall promptly report any significant outsourcing arrangements, major issues, breaches, or termination of material outsourcing contracts to the RBI, as mandated by the applicable Master Directions.
- **Record Keeping:** Maintain meticulous records of all outsourcing agreements, due diligence reports, risk assessments, monitoring reports, and communications with service providers.

13. Internal Controls and Audit

Robust internal controls and independent audit mechanisms shall be in place to ensure the integrity and effectiveness of the outsourcing framework.

- **Internal Control System:** Implement a strong internal control system, including appropriate checks and balances, reconciliation procedures, and authorization limits, for all outsourced activities.
- **Internal Audit:** The Company's internal audit function shall periodically audit the outsourcing process, including vendor selection, contract management, ongoing monitoring, risk management, and compliance with this Policy and regulatory guidelines. The frequency and scope of audit shall be commensurate with the materiality and risk of the outsourced activity.
- **External Audit:** External auditors shall also review aspects of outsourcing as part of their financial statement audit or other specific engagements.

14. Policy Review and Amendment

This Outsourcing Policy shall be a dynamic document, subject to regular review and necessary amendments to maintain its effectiveness and alignment with the evolving regulatory landscape and business environment.

- **Review Frequency:** This Policy shall be reviewed at least **annually** by the Risk Management Department and/or the Compliance Department, in consultation with relevant business functions and the Legal Department.
- **Triggers for Immediate Review:** The Policy shall also be reviewed immediately upon the occurrence of any of the following events:
    - Any significant change or amendment in RBI Master Directions on Outsourcing or other relevant regulations (e.g., SBR, IT Framework).
    - Any major internal organizational change impacting the outsourcing strategy or operations.
    - Significant incidents (e.g., data breach, prolonged service disruption) related to an outsourced activity.
    - Introduction of new types of outsourced services or material changes to existing ones.
    - Findings from internal or external audits indicating systemic deficiencies in the outsourcing framework.
- **Approval:** Any amendments or revisions to this Policy shall be thoroughly reviewed by the Senior Management and/or the Audit Committee (if applicable), and subsequently approved by the **Board of Directors**.
- **Communication:** All approved changes to this Policy shall be promptly communicated to all relevant employees, departments, and stakeholders involved in the outsourcing process.