OUTSOURCING POLICY

LOGIX CORPORATE SOLUTIONS PRIVATE LIMITED

POLICY PARTICULARS	
Particulars	**Details**
Policy Name	Outsourcing Policy
Owner	Compliance Department
Approved By	Board of Directors
Review Frequency	Annual or as and when required by RBI
Version	1.0

1. PREAMBLE

Logix Corporate Solutions Private Limited ("the Company") recognises that outsourcing of certain activities can enhance operational efficiency, improve service quality and enable access to specialised expertise. However, outsourcing also exposes the Company to operational, legal, compliance, strategic, concentration, cyber security and reputational risks.

Accordingly, this Policy has been framed to establish a comprehensive governance framework for outsourcing arrangements while ensuring that outsourcing does not diminish the Company's responsibility towards its customers, regulators or other stakeholders.

The Company shall ensure that outsourcing arrangements are undertaken in a prudent manner consistent with applicable laws, regulations and the Company's risk appetite.

2. OBJECTIVE

The objective of this Policy is to establish a comprehensive framework governing the outsourcing of activities undertaken by Logix NBFC Limited in a manner that is prudent, transparent and compliant with applicable regulatory requirements. The Policy seeks to ensure compliance with the directions and guidelines issued by the Reserve Bank of India (RBI) from time to time, while safeguarding the interests of customers and maintaining the confidentiality, integrity and security of customer information. It further aims to establish an effective governance, approval, oversight and monitoring mechanism for all outsourcing arrangements so as to ensure appropriate accountability and risk management.

The Policy is designed to identify, assess and mitigate operational, legal, compliance, information security, cyber security, strategic and reputational risks associated with outsourcing, while ensuring uninterrupted delivery of outsourced services through robust business continuity arrangements. Additionally, the Policy provides a structured framework for due diligence, performance monitoring and periodic review of service providers, and lays down an effective exit strategy to facilitate the orderly termination or transition of outsourcing arrangements without adversely affecting the Company's operations, regulatory compliance or customer service.

3. REGULATORY FRAMEWORK

This Policy has been formulated in accordance with the applicable provisions of the Reserve Bank of India Act, 1934, the Companies Act, 2013 and the rules made thereunder, the Reserve Bank of India (Non-Banking Financial Company – Scale Based Regulation) Directions, 2023, as amended from time to time, and the RBI Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by NBFCs. The Policy also takes into consideration the provisions of the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, wherever applicable, and all other circulars, notifications, directions, guidelines or instructions issued by the Reserve Bank of India or any other statutory or regulatory authority from time to time. In the event of any inconsistency between this Policy and the applicable laws or regulatory directions, the provisions of such laws,

regulations or directions shall prevail, and this Policy shall be deemed to have been modified to the extent necessary to ensure compliance.

3.1 Regulatory Compliance

The Company shall ensure that all outsourcing arrangements are undertaken in compliance with the applicable regulatory requirements and shall not outsource any activity in a manner that impairs its ability to fulfil its obligations towards customers or the Reserve Bank of India. Outsourcing shall neither diminish the Company's responsibility and accountability for the outsourced activity nor impede effective supervision by the Reserve Bank of India.

In case of any conflict between this Policy and RBI directions, the RBI directions shall prevail.

4. APPLICABILITY

This Policy shall apply to:

- Logix Corporate Solutions Private Limited.
- All departments proposing outsourcing.
- All outsourcing arrangements involving financial services.
- Existing as well as future outsourcing arrangements.

The Policy shall also apply to material outsourcing arrangements executed with group companies or related parties.

5. DEFINITIONS

5.1 Outsourcing

Outsourcing means the engagement of a third party by the Company to perform activities on a continuing basis which would otherwise be undertaken by the Company itself.

5.2 Service Provider

Any person, company, LLP, partnership firm or entity engaged for providing outsourced services.

5.3 Material Outsourcing

Material outsourcing refers to outsourcing arrangements where disruption may materially affect:

- business operations;
- regulatory compliance;
- financial condition;
- customer services;
- reputation of the Company.

5.4 Customer Information

Customer Information includes:

- Personal Information
- Financial Information
- KYC records
- Loan details
- Transaction data
- Credit information
- Account statements
- Authentication credentials

5.5 Board

Board means the Board of Directors of Logix NBFC Limited.

5.6 Senior Management

Senior Management includes Managing Director, Chief Executive Officer and Key Managerial Personnel responsible for implementation of this Policy.

6. SCOPE OF OUTSOURCING

The Company may outsource permissible business and support activities, including loan sourcing support, collection support, customer care, call centre operations, document digitisation, data processing, IT and cloud services, record management, payroll and HR support, legal documentation, recovery support, field verification, technical valuation and other administrative services, in accordance with applicable laws and RBI guidelines. However, outsourcing shall not diminish the Company's responsibility or accountability, and all statutory and regulatory obligations shall continue to remain with the Company.

7. ACTIVITIES WHICH SHALL NOT BE OUTSOURCED

The Company shall not outsource its core management functions or activities requiring the exercise of independent judgment and oversight. These include, but are not limited to, final decision-making in respect of loan sanctions, credit appraisal and approval, risk acceptance, investment decisions and regulatory reporting; functions exclusively entrusted to the Board of Directors such as corporate governance, policy formulation and approval, oversight of internal controls and risk management; compliance functions including regulatory compliance monitoring, statutory certifications and fulfilment of statutory obligations; and the independent internal audit function. The ultimate responsibility and accountability for these activities shall at all times remain with the Company and its Board of Directors.

8. GUIDING PRINCIPLES

All outsourcing arrangements shall be governed by the principles of accountability, customer protection, confidentiality, compliance, transparency and a risk-based approach. The Company shall remain fully responsible and accountable for all outsourced activities and shall ensure that customer interests are adequately protected. Confidentiality and security of customer information shall be maintained at all times, and outsourcing arrangements shall comply with applicable laws, RBI directions and the Company's internal policies. The roles, responsibilities and performance expectations of the service provider shall be clearly defined in the outsourcing agreement. Further, material outsourcing arrangements shall be subject to enhanced due diligence, monitoring and oversight to effectively identify, assess and mitigate associated risks.

9. GOVERNANCE FRAMEWORK

Effective governance is essential to ensure that outsourcing arrangements remain consistent with the Company's strategic objectives and risk appetite.

The governance structure shall include:

- Board of Directors
- Senior Management
- Compliance Function
- Risk Management Function
- Internal Audit
- Business Departments

Each function shall have clearly defined responsibilities.

10. ROLE OF THE BOARD OF DIRECTORS

The Board of Directors shall have the overall responsibility for approving and overseeing the Company's outsourcing framework. The Board shall approve this Policy and review it at least annually or whenever required due to regulatory or business changes. It shall approve all material outsourcing arrangements, ensure the establishment of an effective risk management and internal control framework, and periodically review reports on outsourcing risks and performance. The Board shall oversee compliance with applicable RBI directions, safeguard customer interests, review significant outsourcing failures or incidents, monitor concentration risks arising from outsourcing arrangements, and ensure that outsourcing does not adversely affect the Company's operations, regulatory compliance or reputation.

11. ROLE OF SENIOR MANAGEMENT

Senior Management shall be responsible for the effective implementation of this Policy and for establishing appropriate internal procedures and controls for managing outsourcing arrangements. It shall identify and assess outsourcing risks, conduct due diligence of service providers, ensure execution of legally enforceable outsourcing agreements, and continuously monitor the performance and compliance of service providers. Senior Management shall also maintain complete records of all outsourcing arrangements, ensure the effectiveness of

business continuity and disaster recovery measures, promptly report material outsourcing risks, incidents or non-compliance to the Board of Directors, and take appropriate corrective actions to ensure that all outsourcing activities remain compliant with applicable laws, regulatory requirements and the Company's internal policies.

12. ROLE OF THE COMPLIANCE OFFICER

The Compliance Officer shall:

- monitor compliance with RBI directions;
- review outsourcing agreements;
- advise business departments;
- coordinate regulatory inspections;
- maintain regulatory correspondence;
- report non-compliance to Senior Management.

13. RISK ASSESSMENT FRAMEWORK

13.1 General

Prior to entering into any outsourcing arrangement, the Company shall undertake a comprehensive risk assessment to identify, measure, monitor and mitigate the risks associated with outsourcing. The objective of the assessment is to ensure that outsourcing does not adversely affect the Company's operational resilience, regulatory compliance, financial soundness, or reputation.

The assessment shall be proportionate to the nature, complexity and materiality of the outsourced activity.

13.2 Risks Associated with Outsourcing

The Company shall evaluate, inter alia, the following risks:

a. Strategic Risk

Risk arising from inappropriate business decisions, inadequate implementation of decisions or failure to respond to changes in the business environment due to dependence on the service provider.

b. Operational Risk

Risk of loss resulting from inadequate or failed internal processes, systems, human errors or external events affecting outsourced operations.

c. Compliance and Legal Risk

Risk arising from non-compliance with applicable laws, regulations, RBI directions, contractual obligations or industry standards by the service provider.

d. Reputational Risk

Risk of negative public opinion resulting from poor performance, misconduct or failure of the service provider.

e. Information Security Risk

Risk relating to unauthorised access, disclosure, alteration or destruction of confidential information, customer data or business information.

f. Cyber Security Risk

Risk arising from cyber-attacks, ransomware, malware, phishing, denial of service attacks or compromise of information systems maintained by the service provider.

g. Concentration Risk

Risk arising from excessive dependence on a single service provider or concentration of outsourcing arrangements within a particular geographical region or group entity.

h. Country Risk

Where services are outsourced outside India, the Company shall evaluate the political, economic, legal and regulatory environment of the foreign jurisdiction.

14. MATERIAL OUTSOURCING

An outsourcing arrangement shall ordinarily be considered material where disruption of the outsourced activity could:

- materially impact customer service;
- adversely affect business operations;
- result in regulatory non-compliance;
- cause significant financial loss;
- impair the Company's reputation;
- compromise confidentiality of customer information; or
- adversely affect business continuity.

Material outsourcing arrangements shall require enhanced due diligence, approval and continuous monitoring.

15. DUE DILIGENCE OF SERVICE PROVIDERS

Before entering into any outsourcing arrangement, the Company shall conduct appropriate due diligence to assess whether the proposed service provider possesses the financial strength, operational capability, technical expertise and regulatory compliance necessary to perform the outsourced activities in a safe, efficient and reliable manner. The extent of due

diligence shall be commensurate with the nature, complexity and materiality of the outsourced activity.

15.1 Financial Assessment

The Company shall evaluate the financial soundness of the service provider by reviewing its audited financial statements for the preceding three financial years, net worth, profitability, liquidity position, creditworthiness and any pending insolvency or bankruptcy proceedings, so as to assess its ability to provide uninterrupted services throughout the tenure of the outsourcing arrangement.

15.2 Legal and Regulatory Assessment

The Company shall verify the legal status and regulatory compliance of the service provider, including its constitutional documents, statutory registrations and licences, PAN, GST registration, compliance with applicable labour and other laws, litigation history and any regulatory actions, penalties or proceedings that may have a bearing on the outsourcing arrangement.

15.3 Operational Capability

The Company shall assess the operational capability of the service provider, including its organisational structure, management competence, technical expertise, staffing, infrastructure, business experience, quality certifications, internal control framework and overall capacity to perform the outsourced services efficiently and in accordance with the agreed service levels.

15.4 Information Security Assessment

Where the outsourced activity involves access to customer information or information systems, the Company shall evaluate the adequacy of the service provider's information security and cyber security framework, including access controls, encryption mechanisms, vulnerability management practices, incident response procedures, data protection measures and business continuity and disaster recovery arrangements.

15.5 Reputation Assessment

The Company shall also assess the reputation and integrity of the service provider by considering its market standing, customer references, complaint history, media reports, litigation record, fraud history and any other information relevant to determining its reliability and suitability for the proposed outsourcing arrangement.

16. APPROVAL PROCESS

Every outsourcing proposal shall be subject to an appropriate approval process to ensure that the proposed arrangement is consistent with the Company's business objectives, risk

management framework and applicable regulatory requirements. The concerned business department shall initiate the proposal by preparing a detailed note setting out the scope of services, business justification, estimated cost, risk assessment and details of the proposed service provider. Thereafter, the Compliance Department shall examine the proposal from a regulatory perspective to ensure compliance with applicable laws, RBI directions and the Company's internal policies. The Risk Management Function shall assess the operational, legal, information security, concentration and business continuity risks associated with the proposed outsourcing arrangement and recommend appropriate risk mitigation measures. The Legal Department shall review the proposed outsourcing agreement to ensure that it adequately addresses contractual obligations, liabilities, confidentiality, data protection, audit rights, regulatory access and other applicable legal requirements. Upon completion of these reviews, the proposal shall be placed before the competent approving authority for approval in accordance with the delegation of powers prescribed by the Company.

Approving Authority

Nature of Outsourcing	Approving Authority
Routine administrative or support outsourcing	Functional Head
Material outsourcing arrangements	Managing Director / Chief Executive Officer
Critical or material outsourcing affecting core financial services or having significant regulatory, operational or reputational impact	Board of Directors

17. OUTSOURCING AGREEMENT

Every outsourcing arrangement shall be governed by a comprehensive written agreement executed between the Company and the service provider and approved by the competent authority. The agreement shall clearly define the scope of services, roles and responsibilities of the parties, service standards, rights, obligations, performance expectations and accountability mechanisms. The agreement shall ensure compliance with applicable laws, RBI directions and the Company's internal policies, and shall adequately protect the Company's legal, operational, regulatory and reputational interests.

17.1 Mandatory Clauses

Every outsourcing agreement shall, at a minimum, include provisions relating to the scope of services, service levels and performance standards, fees and payment terms, confidentiality of customer and Company information, ownership of data, compliance with applicable laws, RBI directions and the Company's policies, audit and inspection rights of the Company, its internal and statutory auditors and the Reserve Bank of India, sub-outsourcing restrictions, business continuity and disaster recovery arrangements, reporting of frauds, cyber incidents and security breaches, indemnity for losses arising from the service provider's acts or omissions, and termination rights. The agreement

shall also provide the Company with the right to terminate the outsourcing arrangement in the event of material breach of contract, regulatory non-compliance, fraud, persistent poor performance, insolvency of the service provider, data breach, breach of confidentiality or any other circumstance that may adversely affect the interests of the Company or its customers.

17.2 Minimum Contractual Requirements

Without prejudice to the generality of the foregoing, every outsourcing agreement shall specifically provide for:

- a clear description of the outsourced services and applicable service levels;
- the fees, payment terms and commercial arrangements;
- confidentiality and protection of customer information and Company data;
- ownership and return of all records, documents and data upon termination of the agreement;
- compliance with all applicable laws, RBI directions and Company policies;
- unrestricted access for the Company, its auditors and the Reserve Bank of India to relevant records, systems, premises and personnel for audit or inspection purposes;
- restrictions on sub-outsourcing without the prior written approval of the Company;
- maintenance and periodic testing of business continuity and disaster recovery arrangements;
- immediate reporting of frauds, cyber incidents, operational disruptions or security breaches;
- appropriate indemnity and limitation of liability provisions; and
- termination, transition assistance and orderly transfer of the outsourced activities to the Company or another service provider, without disruption to customers or business operations.

18. CONFIDENTIALITY AND DATA PROTECTION

The Company shall ensure that customer information remains secure throughout the outsourcing lifecycle.

The service provider shall:

- use customer information only for authorised purposes;
- maintain confidentiality;
- implement adequate technical and organisational safeguards;
- restrict access on a need-to-know basis;
- comply with applicable data protection laws;
- immediately report any data breach.

The service provider shall not disclose customer information to any third party without prior written approval of the Company unless required by law.

19. INFORMATION SECURITY

The service provider shall establish and maintain an appropriate information security framework commensurate with the nature, scope and sensitivity of the outsourced activities. Such framework shall ensure the confidentiality, integrity and availability of the Company's and customers' information and shall include adequate administrative, technical and physical safeguards to prevent unauthorized access, disclosure, alteration, loss or misuse of information. The service provider shall, at a minimum, implement appropriate access controls, password management policies, encryption mechanisms, antivirus and malware protection, firewall security, endpoint protection, vulnerability assessment and penetration testing, secure software development practices (where applicable), continuous security monitoring and log management. The Company may periodically review or audit the effectiveness of these controls and require the service provider to promptly address any identified security gaps or vulnerabilities.

20. CYBER SECURITY

Where the outsourced activities involve information technology systems, digital platforms or access to customer information, the Company shall ensure that the service provider maintains adequate cyber security controls and complies with applicable RBI directions and the Company's information security requirements. The service provider shall promptly report any cyber incident, data breach or security compromise to the Company, extend full cooperation during investigation and regulatory reporting, preserve all relevant evidence, implement timely corrective and preventive measures, and periodically review and strengthen its cyber security controls to safeguard the confidentiality, integrity and availability of the Company's information and systems.

21. BUSINESS CONTINUITY AND DISASTER RECOVERY

The Company shall ensure that every material service provider maintains adequate and documented Business Continuity Plan (BCP) and Disaster Recovery (DR) arrangements to ensure uninterrupted delivery of outsourced services during any disruption or emergency. The Company may periodically review, assess or test the effectiveness of such arrangements, wherever considered necessary. The service provider shall maintain appropriate backup facilities, conduct periodic disaster recovery testing, ensure the availability of alternate processing or operational facilities, and establish documented recovery procedures to restore critical operations within agreed timelines. Any failure by the service provider to maintain effective business continuity and disaster recovery arrangements or to comply with the agreed service levels shall constitute a material breach of the outsourcing agreement and may result in termination of the arrangement in accordance with its terms.

The Company shall ensure that adequate contingency measures and an appropriate exit strategy are in place to enable the continuity of critical outsourced services in the

event of service disruption, termination of the outsourcing arrangement or failure of the service provider. The Company shall retain the capability to ensure uninterrupted customer service and compliance with applicable regulatory requirements at all times.