

# OUTSOURCING POLICY

(For Base Layer NBFC – Investment and Credit Company)

## 1. Preamble

This Outsourcing Policy is framed in accordance with:

- Master Direction – Managing Risks and Code of Conduct in Outsourcing of Financial Services by NBFCs issued by the Reserve Bank of India (November 9, 2017, as amended *up to date*)
- *Master Direction on Outsourcing of Information Technology Services, 2023*
- *Guidelines on Digital Lending (2022) regarding Lending Service Providers (LSPs) and Digital Lending Apps (DLAs)*
- RBI Scale Based Regulation (SBR) Framework for NBFCs
- Applicable provisions of the Companies Act, 2013 (*including Sections 134, 177, and 188*)
- Information Technology Act, 2000 and allied Rules
- *The Digital Personal Data Protection (DPDP) Act, 2023*
- RBI Guidelines on IT Governance, Information Security and Cyber Risk Management (as applicable)

Outsourcing arrangements may improve efficiency and specialization; however, they introduce operational, compliance, legal, concentration, reputational, and strategic risks.

This Policy establishes a structured governance, control, monitoring and risk management framework to ensure outsourcing does not compromise regulatory compliance or customer interests.

## 2. Objectives

The objectives of this Policy are to:

- Establish a robust outsourcing governance framework.
- Ensure full compliance with RBI outsourcing directions applicable to NBFC–Base Layer entities.
- Protect customer data, confidentiality and service quality *in strict adherence to the DPDP Act, 2023*.
- Clearly define approval, monitoring and reporting responsibilities.
- Mitigate risks arising from outsourcing arrangements.
- Ensure continuity of critical operations under adverse conditions.
- *Ensure that core management functions and statutory responsibilities are never outsourced.*

## 3. Applicability

This Policy applies to:

- All departments and branches of the Company

- All outsourcing arrangements involving financial, *technology (IT)*, and support services
- Domestic and cross-border outsourcing arrangements
- All employees involved in vendor engagement or monitoring
- *Direct Selling Agents (DSAs), Direct Marketing Agents (DMAs), Recovery Agents, and Lending Service Providers (LSPs).*

## 4. Definition and limitations of outsourcing

Outsourcing refers to an arrangement where the Company engages a third party to perform activities on a continuing basis that would otherwise be undertaken by the Company.

### Outsourcing includes:

- Loan sourcing and processing
- Collection and recovery services
- IT operations, *cloud services*, and system maintenance
- Call centre operations
- Data processing and storage
- Field verification
- Tele-marketing

### Activities that **SHALL NOT** be outsourced (Core Management Functions):

*The Company shall not outsource core management functions including:*

1. *Internal Audit and Compliance function.*
2. *Decision-making functions like determining compliance with KYC norms for opening deposit accounts (if applicable) or loan origination.*
3. *Sanctioning of loans.*
4. *Management of investment portfolio.*

### It excludes:

- Purchase of standard software or hardware
- Professional advisory services (legal, audit, tax consultants)
- Utilities and facility management
- *Clearing and settlement arrangements*

## 5. Board approved governance structure

### 5.1 Role of the Board

The Board shall, *in alignment with its duties under Section 134 of the Companies Act, 2013:*

- Approve the Outsourcing Policy.
- Approve outsourcing of critical activities.
- Review outsourcing risk exposure annually.
- Ensure adequate internal control and oversight mechanisms.
- Ensure compliance with RBI directions.

The Board retains ultimate responsibility for outsourced functions *and customer grievance redressal*.

## 5.2 Role of Senior Management

Senior Management shall:

- Identify outsourcing requirements.
- Conduct due diligence before vendor onboarding.
- Ensure contract execution with appropriate safeguards.
- Monitor vendor performance and compliance.
- Report material risks to the Board.
- *Ensure independent audits of the outsourced service providers.*

## 5.3 Outsourcing Oversight Committee (If Constituted)

The Company may constitute a management-level committee (*or utilize the Audit Committee as per Section 177 of the Companies Act, 2013*) to:

- Review critical outsourcing arrangements
- Assess vendor risk profile
- Monitor concentration risk
- Review performance deviations
- *Approve related party outsourcing transactions at arm's length pricing (Section 188 of Companies Act, 2013).*

# 6. Risk-based approach to outsourcing

Outsourcing decisions shall be guided by risk assessment covering:

- Operational Risk
- Compliance Risk
- Strategic Risk
- Reputational Risk
- Data Security *and Privacy Risk (DPDP Act compliance)*
- Concentration Risk
- Legal Risk

A documented risk assessment note shall precede outsourcing approval.

# 7. Classification of outsourced activities

## 7.1 Critical Activities

An activity shall be considered critical if disruption would:

- Materially affect business operations
- Impact customer service significantly
- Lead to regulatory breach
- Cause reputational damage

- Affect financial position

Examples: Core IT systems, Loan management software, Collection and recovery operations, Customer database management. Critical outsourcing requires enhanced monitoring and Board visibility.

## 7.2 Non-Critical Activities

Support services with limited systemic impact.

# 8. Vendor due diligence framework

Prior to entering into any outsourcing agreement, the Company shall conduct comprehensive due diligence covering:

## 8.1 Financial Evaluation

- Audited financial statements (last 2–3 years)
- Net worth position
- Profitability trend
- Liquidity adequacy
- Debt profile

## 8.2 Technical & Operational Capability

- Infrastructure adequacy
- IT systems capability
- Skilled manpower
- Disaster recovery readiness
- Data handling practices

## 8.3 Governance & Compliance

- Regulatory track record *and RBI adverse remarks (if any)*
- Litigation history
- Internal control framework
- AML & KYC compliance (if applicable)

## 8.4 Information Security & Privacy Assessment

- Cybersecurity controls
- Encryption mechanisms
- Access control protocols
- Incident response mechanism
- *Data privacy protocols and readiness to act as a 'Data Processor' under the DPDP Act, 2023.*

Due diligence findings must be documented and approved by the designated authority.

# 9. Outsourcing agreement – mandatory clauses

Every outsourcing arrangement must be governed by a written, legally enforceable agreement containing:

## 9.1 Scope and Responsibilities

- Clear definition of services
- Roles and responsibilities
- Performance expectations

### **9.2 Service Level Agreements (SLAs)**

- Measurable performance metrics
- Turnaround time
- Penalty provisions
- Escalation matrix

### **9.3 Confidentiality & Data Protection**

- Data access restrictions
- Encryption requirements
- Compliance with IT laws *and the DPDP Act, 2023*
- Restriction on data sharing
- ***Mandatory clause ensuring all customer data is stored on servers located within India.***

### **9.4 Audit & Inspection Rights**

The Company and the Reserve Bank of India (*or persons authorized by them*) shall have unrestricted access to:

- Books
- Records
- Systems
- Relevant documents

### **9.5 Sub-Contracting**

Sub-outsourcing permitted only with prior written approval of the Company. ***The primary vendor retains full liability for the sub-contractor's actions.***

### **9.6 Business Continuity & Disaster Recovery**

Mandatory BCP & DR testing obligations.

### **9.7 Termination & Exit Management**

Agreement must provide for:

- Termination for regulatory breach
- Immediate termination for data breach
- Transition support
- Data return/destruction (*including certified erasure logs*)

## **10. Data security & confidentiality**

The Company shall ensure:

- Customer data shared strictly on *a need-to-know basis with explicit consent from the customer.*
- Encryption during storage and transmission.
- Restricted role-based access.
- Secure destruction of data post-termination.

- Non-Disclosure Agreement (NDA) shall be mandatory.
- Data breach must be reported immediately to senior management and, if required, to RBI *and CERT-In within mandated timelines (e.g., 6 hours for severe cyber incidents)*.
- *As a Data Fiduciary, the Company holds the outsourced agent (Data Processor) strictly accountable for any data leaks.*

## 11. Monitoring framework

### 11.1 Ongoing Monitoring

- Monthly/Quarterly SLA review
- Performance scorecards
- Complaint tracking (*specifically linking complaints to LSPs/Recovery Agents*)

### 11.2 Periodic Audits

Critical vendors shall be subject to:

- On-site audits
- IT security review
- Compliance audit

Audit observations shall be documented and tracked for closure.

### 11.3 Concentration Risk Monitoring

The Company shall avoid excessive reliance on a single vendor for multiple critical activities.

## 12. Code of conduct for outsourced agents

Outsourced agents interacting with customers (especially collections *and DMAs/DSAs*) must:

- Follow *the Fair Practices Code*.
- Avoid coercive or abusive recovery practices (*including physical or verbal harassment, or accessing the borrower's phone contacts/media*).
- Respect customer dignity.
- Carry valid authorization (*Identity Cards*).
- *Adhere strictly to RBI calling hour regulations (Calls permitted only between 08:00 AM and 07:00 PM)*.
- *Ensure recovery agents undergo mandatory training and certification (e.g., IIBF Debt Recovery Agent certification)*.

The Company remains *fully* responsible for their conduct.

## 13. Business continuity & contingency planning

The Company shall ensure:

- Vendor has *a* tested BCP
- Disaster recovery site for critical IT functions
- Defined recovery time objectives (RTO) *and Recovery Point Objectives (RPO)*
- Internal fallback arrangements
- Periodic testing of BCP shall be documented.

## 14. Incident management

Material incidents include:

- Data breach
- Cyberattack
- System outage
- SLA breach with financial impact
- Regulatory non-compliance

Incident reporting shall include:

- Root cause analysis
- Corrective action
- Preventive action
- *Statutory reporting to RBI and CERT-In.*

## 15. Termination & exit strategy

Upon termination:

- Access credentials revoked
- Data securely returned or destroyed
- Transition plan implemented
- Customer service continuity ensured

Exit risk assessment must be recorded.

## 16. Regulatory reporting

The Company shall:

- Maintain a register of outsourcing arrangements.
- Provide information to RBI during inspection.
- Report material adverse developments to RBI.
- Ensure critical outsourcing remains compliant with RBI directions.
- *Publish the list of active LSPs, DLAs, and Recovery Agents on the Company's official website.*

## 17. Record keeping

The following shall be preserved *as per Section 128 of the Companies Act, 2013 and PMLA requirements*:

- Due diligence reports

- Risk assessment notes
- Agreements and amendments
- SLA reports
- Audit findings
- Incident reports

Retention shall be as per regulatory requirements.

## 18. Internal audit

Internal Audit shall periodically review:

- Compliance with *the* outsourcing policy
- Effectiveness of monitoring controls
- Data security compliance
- Vendor risk management
- Major findings shall be placed before the Board *or the Audit Committee*.

## 19. Policy review

This Policy shall be:

- Reviewed annually
- Updated upon regulatory change
- Approved by the Board

## 20. Effective date

This **OUTSOURCING POLICY** has been approved by the Board of Directors of THIRUKOCHI FINCAP PRIVATE LIMITED at its meeting held on 12/03/2026.

Effective Date: 12/03/2026