

BUSINESS CONTINUITY PLAN (BCP)

(For Base Layer NBFC – Investment and Credit Company)

1. Regulatory Background

Under the RBI's Scale Based Regulation (SBR) Framework (*Master Direction - Reserve Bank of India (Non-Banking Financial Company - Scale Based Regulation) Directions, 2023*), NBFCs classified as Base Layer (NBFC-BL) are required to maintain adequate governance standards, risk management practices, and operational resilience mechanisms.

Furthermore, pursuant to Section 134(3)(n) of the Companies Act, 2013, the Board of Directors is required to oversee a robust risk management policy, encompassing the identification and mitigation of risks that could threaten the existence of the company.

Though regulatory prescriptions for Base Layer entities are proportionate to their size and systemic risk, RBI mandates that all NBFCs must have:

- A documented Business Continuity Plan (BCP)
- Disaster Recovery (DR) arrangements
- Periodic testing of continuity arrangements
- Reporting mechanisms for major disruptions

This BCP is framed to comply with:

- RBI Scale Based Regulation (SBR) for NBFCs
- *RBI Master Direction on Information Technology Framework for the NBFC Sector*
- RBI Master Directions applicable to NBFC-ICC
- RBI expectations on operational resilience
- *Applicable provisions of the Companies Act, 2013 regarding risk governance.*

2. Objective

The objective of this BCP is to:

1. Ensure continuity of critical financial services *and minimize downtime* during disruptions.
2. Minimize financial, operational, *and reputational* losses.
3. Protect customer data, funds, *and corporate assets*.
4. Maintain *strict* regulatory compliance *under RBI and statutory frameworks*.
5. Ensure timely restoration of systems *within predefined recovery timelines*.

3. Applicability

This BCP applies to *all operations of Thirukochi Fincap Limited, encompassing:*

- Head Office *and branch* operations
- Loan origination & disbursement
- Collections & recovery
- Accounting & treasury
- Regulatory reporting
- IT systems (Core Lending System)
- Digital lending operations (if any)
- Outsourced service providers *and third-party vendors integrated into the Company's network*.

4. Governance Framework

4.1 Board Responsibility

In line with the Companies Act, 2013 and RBI IT Governance expectations, the Board shall:

- Approve the *foundational BCP policy and framework*.

- Review the BCP annually *or upon any material change in business operations*.
- Ensure adequate *budgetary allocation* for IT and DR infrastructure.
- Review major incident reports *and post-incident analyses*.
- Ensure *ultimate* compliance with RBI directions.

4.2 Senior Management Responsibility

Senior Management (*including the Crisis Management Team*) shall:

- Implement *and operationalize* the BCP.
- Conduct *and document* periodic testing.
- Maintain *comprehensive* incident logs.
- Ensure timely regulatory reporting *to the RBI and other statutory bodies*.
- *Promote a culture of BCP awareness and readiness among all employees*.

5. Risk Assessment (Base Layer Approach)

As an NBFC-ICC (Base Layer), the Company shall identify proportionate but adequate risk categories *that could trigger a business disruption*:

- **5.1 Natural Risks:** Flood, Fire, Earthquake, Severe weather *events*.
- **5.2 IT & Cyber Risks:** System downtime, Ransomware attacks, Data breaches, Malware infections, Phishing incidents, *and Distributed Denial of Service (DDoS) attacks*.
- **5.3 Operational Risks:** Power failures, Network outages, *Mass* employee unavailability (*e.g., transit strikes*), Pandemic situations.
- **5.4 Vendor Risks:** Data center outages, Core lending system failures, Payment gateway disruptions, *and failure of critical third-party cloud service providers*.

6. Business Impact Analysis (BIA)

The BIA identifies critical functions and establishes their Maximum Tolerable Period of Disruption (MTPD). The following tables outline the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) benchmarks:

Function	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)
Core Lending System	4 Hours	1 Hour
Data Backup	1 Hour	1 Hour
Customer Service	12 Hours	1 Hour
Loan Disbursement	24 Hours	4 Hours
Payment Processing	12 Hours	2 Hours
Regulatory Reporting	48 Hours	24 Hours

Note: Base Layer entities may adopt simplified but clearly documented RTO/RPO benchmarks, *provided they do not compromise customer data integrity or regulatory reporting deadlines*.

7. IT Disaster Recovery (Mandatory for NBFC-BI)

Even for Base Layer, RBI expects a *robust IT recovery mechanism*:

7.1 Data Backup

- Daily automated *and scheduled* backups.
- Encrypted offsite backup (*preferably located in a different seismic zone to prevent simultaneous destruction*).
- Periodic restore testing *to verify data integrity*.
- *Secure maintenance of Backup logs*.

7.2 Disaster Recovery Arrangement

- Secondary server environment, OR
- Cloud-based redundancy (*multi-availability zones*), OR

- DR vendor arrangement.
- *The recovery capability must strictly meet the defined RTO/RPO parameters.*

8. Cyber security controls

As per RBI expectations *for maintaining operational resilience*:

- Firewall protection *and Intrusion Detection/Prevention Systems (IDS/IPS).*
- Antivirus & endpoint security *across all corporate devices.*
- *Role-based Access controls (RBAC).*
- *Multi-factor authentication (MFA) for remote access and critical applications.*
- *Periodic vulnerability assessments and penetration testing (VAPT).*
- *A documented Incident response mechanism.*
- *Cyber incidents must be documented and reported to the Indian Computer Emergency Response Team (CERT-In) within 6 hours of identification, alongside standard RBI reporting, where required.*

9. Crisis management structure

A dedicated Crisis Management Team (CMT) shall be constituted to manage disruptions:

- **Managing Director** – BCP Head (*Ultimate operational authority*)
- **Head of IT** – System Recovery (*Technical restoration*)
- **Compliance Officer** – Regulatory Communication (*Liaison with RBI/Statutory bodies*)
- **HR Head** – Employee Safety (*Staff communications and welfare*)

CMT responsibilities:

- *Assess incident severity and impact.*
- *Activate the relevant phases of the BCP.*
- *Allocate emergency responsibilities.*
- *Escalate critical matters to the Board.*

10. Incident activation criteria

The BCP shall be activated when:

- *System downtime exceeds the defined threshold (e.g., > 4 hours).*
- *A verifiable data compromise occurs.*
- *Office premises become inaccessible for prolonged periods.*
- *Regulatory reporting or core payment capabilities are disrupted.*

Severity levels:

- **Level 1 – Minor incident:** *Resolved within standard operational procedures; local impact.*
- **Level 2 – Major disruption:** *Requires BCP activation; impacts multiple departments or customer-facing services.*
- **Level 3 – Critical incident:** *Severe threat to business viability; requires immediate Board escalation and RBI notification.*

11. Regulatory Reporting

For significant disruptions (*Level 2 and Level 3*), the Company shall:

- *Inform the respective RBI Regional Office (Department of Supervision).*
- *Submit a preliminary incident report.*
- *Provide periodic status updates.*
- *Submit a comprehensive Root Cause Analysis (RCA) and closure report.*
- *The Compliance Officer shall maintain a formal record of all regulatory communication.*

12. Alternate work arrangements

Base Layer NBFCs must ensure *operational flexibility through:*

- *Work-from-home capability for critical staff.*
- *Secure VPN access with end-to-end encryption.*
- *Alternate office space arrangement (if feasible or required by business volume).*

13. Vendor continuity management

To mitigate third-party dependencies, the Company shall:

- Obtain a formal BCP declaration from all critical vendors.
- Include mandatory business continuity and right-to-audit clauses in Service Level Agreements (SLAs).
- Review vendor DR readiness and test results on an annual basis.

14. Testing requirement (Mandatory)

As per regulatory expectation, the Company commits to:

- Annual BCP tabletop or functional testing.
- Disaster Recovery failover drill.
- Formal documentation of results.
- Gap analysis report identifying vulnerabilities during the test.
- Corrective action plan with assigned timelines.
- Submission of the final Test results to be placed before the Board for review.

15. Documentation & record keeping

Maintain and secure the following in a centralized repository:

- The approved BCP document.
- Incident logs and resolution reports.
- DR test reports and sign-offs.
- Vendor BCP certifications.
- RBI and statutory communication records.

16. Policy review

This BCP shall be:

- Reviewed annually by the Risk Management Committee / Board.
- Updated upon any significant operational shift or regulatory change.
- Approved by the Board of Directors.

17. Proportionality for Base Layer

While the regulatory burden is lower than that of Middle and Upper Layer NBFCs, the Company shall diligently ensure:

- Basic but effective DR arrangement.
- Clear recovery timelines (RTO/RPO).
- Adequate data protection and privacy protocols.
- Active Board oversight.
- Documented and verifiable testing.

18. Effective date and approval

This **BUSINESS CONTINUITY PLAN (BCP)** has been approved by the Board of Directors of **THIRUKOCHI FINCAP LIMITED** at its meeting held on **12/03/2026**.

This policy supersedes any previous business continuity frameworks and is binding on all employees and designated stakeholders.

Effective Date: 12/03/2026.

Version:1