RISK & FRAUD MANAGEMENT POLICY

Identify. Prevent. Protect.

APPLICABLE TO: BOARD, RISK MANAGEMENT COMMITTEE, ALL EMPLOYEES & BUSINESS OPERATIONS

Department: Risk Management / Compliance

CONFIDENTIAL — FOR INTERNAL / BOARD / REGULATOR USE

SABRIMALA FINTECH PRIVATE LIMITED

1. PURPOSE & OBJECTIVES

Sabrimala Fintech Private Limited ("the Company") is a non-deposit taking NBFC – Investment and Credit Company registered with the Reserve Bank of India ("RBI") and classified in the Base Layer ("NBFC-BL"). It offers four credit products, each with a distinct risk profile:

Unsecured SME Loans — Credit-assessment, fraud and collection risk.
Gold Loans — Collateral-price, custody and assaying risk.
Loan Against Property (LAP) — Legal, valuation and enforcement risk.
Non-Income-Proof (NIP) Loans — Credit-assessment, fraud and collection risk for informal-sector borrowers.

This Risk & Fraud Management Policy ("the Policy") combines the Company's Risk Management Policy and Fraud Risk Management Policy into a single Board-approved framework. Its objectives are to:

- Identify, measure, monitor, mitigate and report all material risks across products and the Company as a whole.
- Constitute the Risk Management Committee required under the RBI (NBFC – Governance) Directions, 2025.
- Set risk appetite, exposure limits and early-warning triggers specific to the Company's four products.
- Prevent, detect, report and manage fraud with a zero-tolerance approach.
- Define risk ownership, escalation paths and the frequency of reporting to the RMC and the Board.

2. SCOPE

This Policy applies to the Board of Directors, the Risk Management Committee, all permanent and contractual employees, trainees, branch and field staff, authorised agents, vendors and third-party service providers. It covers loan sourcing, onboarding, credit appraisal, documentation, disbursement, collections, custody of collateral, financial transactions, technology and all other business activities.

3. REGULATORY FRAMEWORK

This Policy is framed with reference to the consolidated RBI Master Directions for NBFCs issued on 28 November 2025 (as updated), including:

RBI DIRECTION	RELEVANCE TO THIS POLICY
NBFC – Governance Directions, 2025 (para. 9)	Mandatory Risk Management Committee; evaluates overall risk including liquidity risk and reports to the Board
NBFC – Credit Risk Management Directions, 2025	Board-approved credit risk policy, appraisal standards, LEI for large borrowers, monitoring of stressed accounts
NBFC – Concentration Risk Management Directions, 2025	Single-borrower / group limits and sub-segment limits, particularly for unsecured exposures
NBFC – Asset Liability Management Directions, 2025	Liquidity risk framework and structural liquidity monitoring
NBFC – IRACP Directions, 2025	SMA / NPA classification (90-day norm) and provisioning
Lending Against Gold and Silver Collateral Directions, 2025	Tiered LTV ceilings, assaying, custody, collateral return and auction norms
Credit Facilities and Responsible Business Conduct Directions, 2025	Loan documentation, KFS, penal-charge rules and collection conduct
Managing Risks in Outsourcing Directions, 2025	Valuers, assayers, collection agents, DSAs and technology vendors
KYC Directions, 2025	KYC / AML risk, including scrutiny of gold collateral ownership
Cybersecurity, Technology Risk, Resilience and Assurance Framework Directions, 2026	Technology and cyber risk for Base Layer NBFCs
Master Directions on Fraud Risk Management	Fraud risk framework, adopted proportionately (mandatory scope presently covers NBFCs-BL with assets of ₹500 crore and above)

NOTE

The Scale Based Regulation Master Direction of October 2023 stands repealed from 28 November 2025. The 90-day NPA norm applies to the Company in full from 31 March 2026. The Compliance Officer shall verify the "Updated as on" date of each Direction before every annual review.

4. RISK GOVERNANCE STRUCTURE

The Company follows a three-lines model, scaled to its size:

LINE	WHO	ROLE
First line – Risk owners	Branch and regional teams; Credit Head / COO; Gold Loan operations; Collections	Originate and manage exposures within approved limits; execute controls; raise early-warning flags
Second line – Risk oversight	Risk Function (Head – Risk); Compliance Officer; MIS	Design and monitor limits and triggers; independent review of credit, collateral and liquidity risk; prepare the RMC dashboard
Third line – Assurance	Internal Audit (Senior Manager); Statutory Auditor	Independent testing of the risk framework; reporting to the RMC and the Board

LINE	WHO	ROLE
Oversight	Risk Management Committee; Board of Directors	Approve risk appetite and this Policy; review the risk profile at least quarterly; direct corrective action

Head – Risk

A Chief Risk Officer is not mandatory for the Company (required only above ₹5,000 crore assets). The Board has designated Mr. Rupak Dassarma (Head – Operation) & Chirag Thakkar (Head – Credit) as Head – Risk, reporting functionally to the RMC and administratively to the Managing Director & Director. The Head – Risk shall not carry business targets, shall have unrestricted access to credit files, collateral records and MIS, and shall attend every RMC meeting.

5. RISK MANAGEMENT COMMITTEE (RMC)

The Board constitutes a Board-level RMC of not less than three members, with a majority of non-executive directors and a non-executive Chairperson experienced in banking, NBFC operations or risk management.

MEMBER	DIN	BOARD DESIGNATION	RMC ROLE
Mr. Prakash Chandra Sahoo	07613123	Non-Executive Director	Chairperson
Mr. Arun Dash	07972670	Non-Executive Director	Member
Mr. Jayeshkumar Shankarji Solanki	10821641	Director	Member
Mr. Ashish Kumar Dash	07565098	Managing Director	Member

Permanent invitees (without voting rights): Dr. Ajit Kumar Sabat, Mr. Ashutosh Mishra, Mr. Murugan Govindaraj (Additional Director), the Head – Operation, Credit, the Compliance Officer and the Senior Manager – Internal Audit. The Company Secretary (or the Compliance Officer) shall act as Secretary to the RMC.

Meetings, Quorum & Minutes

- At least once every calendar quarter (minimum four meetings a year), with not more than 120 days between meetings.
- Quorum: two members or one-third of the strength, whichever is higher, with at least one Non-Executive Director present.
- Agenda and the Risk Dashboard circulated at least 5 working days in advance; minutes circulated to the Board within 15 days.

The Chairperson shall convene a special meeting within 15 days of any of the following triggers:

- A breach of any Board-approved limit in Annexure I.
- A single fraud or suspected fraud of ₹10 lakh or more.
- A movement of more than 10% in the gold price benchmark within 30 days.
- Any RBI inspection observation, direction or penalty relating to risk.
- Any event that materially alters the Company's risk profile.

Key Responsibilities of the RMC

- Evaluate overall risk – credit, concentration, collateral, liquidity, interest-rate, operational, fraud, technology, outsourcing, compliance, conduct and reputational – and report to the Board after every meeting.
- Recommend the risk appetite and Annexure I limits to the Board and review them at least annually.
- Review product-wise portfolio quality (SMA / NPA, provisioning, restructuring, write-offs, collection efficiency) every quarter.
- Oversee liquidity, gold-collateral and LAP-collateral risk, capital adequacy and stress tests.
- Oversee the early-warning and fraud risk framework, including all frauds and attempted frauds, root cause and staff accountability.
- Review outsourcing, technology and cyber risk, compliance status, RBI observations and internal audit findings.
- Review new products, geographies or channels from a risk perspective before Board approval.

The RMC may call for any information, obtain external professional advice, direct suspension of a product, branch or channel pending remediation, and require the Managing Director to present a remediation plan. It shall evaluate its own performance once a year.

6. RISK APPETITE

The Board's risk appetite is moderate. The Company will grow its secured portfolios (Gold and LAP) as the anchor of its balance sheet, extend unsecured SME and NIP credit only within defined sub-limits, maintain a capital buffer above the regulatory minimum, and will not accept risks that could impair its ability to meet obligations to lenders or comply with RBI directions. Quantitative limits are set out in Annexure I.

Any breach of an Annexure I limit shall be escalated as follows:

Head – Risk (same day) → Chairperson, RMC (within 2 working days) → RMC and Board (next meeting, with a remediation plan).

7. CREDIT RISK

General Principles

- Every credit decision is taken under a Board-approved delegation matrix, with maker-checker separation between origination and sanction.
- Every borrower is assessed for identity, capacity, character and collateral, with a credit bureau report for every applicant and co-applicant.
- Loans to directors, relatives, senior officers and related entities follow the Board-approved policy and are reported to the RMC quarterly.
- A Legal Entity Identifier is obtained from non-individual borrowers above the prescribed threshold before any new exposure.
- Restructuring, settlement and write-off follow the Board-approved framework and are reported to the RMC with rationale.

Product-wise Key Controls

PRODUCT	KEY CONTROLS
Loan Against Property	Clear, marketable residential / commercial property only (agricultural, disputed or under-acquisition property ineligible); LTV within Annexure I on the lower of two valuations above the threshold; 30-year title search by an empanelled advocate; registered / equitable mortgage with CERSAI filing; FOIR within limit; property insurance with the Company as loss payee; revaluation on SMA-2 or restructuring.
Gold Loan	18–22 carat ornaments only; LTV within RBI tiered ceilings (85% up to ₹2.5 lakh, 80% up to ₹5 lakh, 75% above ₹5 lakh); bullet loans up to 12 months; standardised assaying in the borrower's presence; proof / declaration of ownership; dual custody, insurance and quarterly surprise checks (10% of packets; 100% annually); collateral returned within 7 working days; auctions as per RBI Directions and the Fair Practices Code.
Unsecured SME Loans	Minimum business vintage as per Credit Policy; banking cash-flow, GST and field verification; surrogate assessment only within sub-limit; per-borrower and group ceilings; repayment through NACH / standing instruction.
Non-Income-Proof Loans	Documented household cash-flow assessment at business / residence, cross-checked with observable indicators and bureau data; dual sign-off above threshold; most tightly limited product; microfinance norms applied where the loan qualifies as a microfinance loan.

8. CONCENTRATION RISK

In line with the RBI (NBFC – Concentration Risk Management) Directions, 2025, the Company sets the following limits (Annexure I), monitored monthly by the Risk Function and reported quarterly to the RMC:

- Single-borrower and single-group ceilings as a percentage of Tier I capital and in absolute amounts.
- Product-wise portfolio ceilings and an aggregate sub-limit for unsecured exposure (SME + NIP).
- Geographic ceilings by state and district / branch cluster, given concentration in Odisha and the National Capital Region.
- Sectoral ceilings within the SME book and a ceiling on gold as a single collateral type, with a gold-price stress trigger.

Any proposal that would breach a limit shall be declined unless the Board has approved a temporary tolerance in advance.

9. LIQUIDITY, INTEREST-RATE & CAPITAL RISK

- Structural liquidity statement prepared at least quarterly, with the short-term negative mismatch kept within the Annexure I tolerance.
- Liquidity buffer of unencumbered cash, bank balances and undrawn committed lines, and a Board-approved contingency funding plan.
- Borrowings diversified across lenders and tenors, with single-lender concentration within the Annexure I ceiling.
- Interest-rate risk measured through a rate-sensitivity gap and earnings-at-risk for a 100 bps parallel shift, reviewed quarterly.
- CRAR maintained above the regulatory minimum with an internal buffer; a four-quarter capital projection presented at each RMC meeting.

10. FRAUD RISK MANAGEMENT

The Company maintains a zero-tolerance approach towards intentional fraud, dishonesty, misrepresentation, corruption and misuse of Company or customer funds.

Zero Tolerance — No intentional fraud, dishonesty or misuse of funds will be accepted at any level.
Fair Examination — All suspected fraud incidents will be examined fairly, confidentially and without prejudice.
Firm Action — Appropriate disciplinary, recovery, legal or regulatory action will be taken where warranted.

Types of Fraud Risk

CATEGORY	EXAMPLES
Loan & Customer-Related	Forged KYC, income or property documents; misrepresentation; fake borrowers or impersonation; manipulated valuation or ownership records; collusion.
Employee & Internal	Misappropriation of collections or funds; unauthorised changes to loan records; kickbacks; misuse of customer data; falsified attendance or expense records.
Digital & Cyber	Phishing, identity theft, unauthorised system access, fraudulent digital payments, manipulation of electronic records, misuse of credentials or OTPs.
Third-Party	Fraudulent verification or valuation reports; misconduct by recovery agents or outsourced providers; vendor collusion.

Prevention & Internal Controls

- KYC and due diligence, independent credit appraisal and verification of income, property and loan documents.
- Segregation of duties between sourcing, verification, sanction and disbursement; defined approval authority and limits.
- Maker-checker on all disbursements and gold-packet movements; dual custody of gold and title documents.
- Daily reconciliation of cash and collateral; periodic reconciliation of collections; restricted system access.
- Collections recorded and deposited within prescribed timelines; no unauthorised settlement, waiver or diversion of funds.

> **IMPORTANT**
> *Employees must not bypass approved procedures, authorise transactions beyond their delegated authority, or conceal, alter or destroy records relating to a suspected fraud.*

Early Warning Signals

The Risk Function shall maintain an early-warning framework that flags, at a minimum:

- First-EMI bounce, unusual changes in bank-account details or behaviour, and borrower unreachable at the recorded address.
- Multiple loans against the same property or gold packet; valuation or purity variance above tolerance on re-assay.
- Inconsistent documents, repeated processing exceptions and multiple applications with common contact details.
- Unexplained collection shortages, delayed deposits or unauthorised loan-account adjustments.

- Unusual employee or vendor behaviour, adverse media, and complaints indicating financial misconduct.

Fraud Reporting & Escalation

Every employee must report suspected or actual fraud promptly, with relevant facts and evidence, through the following path:

Employee → Reporting Manager → Compliance / Risk Function / Designated Fraud Reporting Officer → RMC → Board, and RBI / law-enforcement agencies where applicable.

Where the Reporting Manager is involved, the employee may report directly to HR, Compliance or senior management.

Investigation Process

STEP	ACTION
Step 1	Initial assessment of the complaint or incident and preservation of documents, records and evidence.
Step 2	Investigation by a team independent of the originating branch.
Step 3	Review of transactions, system records and supporting information; opportunity for the person concerned to be heard.
Step 4	Findings and recommendations; classification of confirmed fraud and reporting to the RMC.
Step 5	Management decision on disciplinary, recovery, legal or regulatory action; reporting to RBI and law-enforcement agencies within prescribed timelines, where applicable.

Whistleblower Protection

Employees reporting suspected fraud in good faith shall be protected against retaliation, and their identity kept confidential to the extent reasonably practicable and legally permitted. Knowingly false or malicious allegations may result in disciplinary action.

11. OPERATIONAL, TECHNOLOGY & OUTSOURCING RISK

- Operational risk: each department maintains a risk-and-control self-assessment, reviewed half-yearly; loss events above ₹1 lakh are logged in a loss-event register and reported to the RMC.
- Technology & cyber risk: systems are governed by a Board-approved information security policy (see the Cyber Security Policy); IS audit findings are placed before the RMC and the Board; cyber incidents are reported to RBI within the prescribed timeline.
- Outsourcing risk: valuers, advocates, assayers, DSAs, collection agents and technology vendors are subject to due diligence, written agreements, periodic review and a code of conduct. Core functions such as credit sanction and compliance shall not be outsourced; the outsourcing register is reviewed annually.

12. COMPLIANCE, CONDUCT & REPUTATIONAL RISK

The Compliance Officer maintains a compliance calendar of RBI returns, Companies Act filings and statutory obligations, and reports filing status, RBI correspondence and inspection observations to the RMC every quarter. Conduct risk from mis-selling, opaque pricing, harassment in collection or wrongful auction of gold is mitigated through the Fair Practices Code, Key Facts Statement, Grievance Redressal Policy and the code of conduct for recovery agents.

13. ROLES & RESPONSIBILITIES

All Employees

- Follow approved lending, operational and fraud-prevention procedures, and verify customer information carefully.
- Protect Company assets, customer funds and records; avoid conflicts of interest.
- Report suspicious transactions, misconduct and early-warning signals promptly, and cooperate with investigations.

Branch Managers & Department Heads

- Monitor operations, exceptions and fraud indicators, and ensure compliance with lending and collection procedures.
- Escalate limit breaches and suspected fraud without delay, and support corrective action and staff awareness.

14. RISK REPORTING FRAMEWORK

REPORT	PREPARED BY	RECIPIENT	FREQUENCY
Limit breaches & early-warning exceptions	Risk Function	Head – Operation / Credit; MD	Weekly / as arising
Product-wise portfolio quality	Risk Function with MIS	MD; Operation / Credit Head	Monthly
Gold custody verification & price sensitivity	Gold Loan operations; Internal Audit	Head – Operation / Credit	Monthly / Quarterly
RMC Risk Dashboard	Head – Operation / Credit	RMC	Quarterly
Structural liquidity & interest-rate statements	Finance / Accounts	RMC	Quarterly
Fraud, outsourcing & IS-audit summary	Risk Function; Internal Audit	RMC; Board	Quarterly
RMC report to the Board	Chairperson, RMC	Board of Directors	After every RMC meeting
Review of risk appetite, limits & this Policy	Head – Risk; Compliance Officer	RMC; Board	Annually

15. DISCIPLINARY & CORRECTIVE ACTION

Any person found responsible for fraud, deliberate breach of limits or procedures, manipulation of records or concealment of risk events may face action proportionate to the misconduct, including warning, suspension or termination, recovery of losses through lawful procedures, termination of vendor relationships, civil or criminal proceedings, and reporting to regulatory authorities.

16. REVIEW & AMENDMENT

This Policy and its Annexure shall be reviewed by the RMC and approved by the Board at least once every financial year, and earlier on any amendment to the RBI Directions, a change in layer classification or the introduction of a new

product. Changes made for immediate regulatory compliance shall be ratified at the next Board meeting. In case of conflict, RBI directions shall prevail; for customer-facing conduct, the Fair Practices Code shall govern.

ANNEXURE I — RISK APPETITE LIMITS

PARAMETER	BOARD-APPROVED LIMIT / TOLERANCE
Capital adequacy	CRAR not less than 15% (regulatory minimum) plus an internal buffer of 3%; Tier I not less than 10%
Single borrower exposure	Not more than 25% of Tier I capital, and in any case not more than ₹250 lakh
Single group exposure	Not more than 25% of Tier I capital
LAP portfolio	Not more than 20% of AUM; LTV up to 60% (residential) and 50% (commercial); two valuations above ₹20 lakh; FOIR not exceeding 60%
Gold Loan portfolio	Not more than 20% of AUM; LTV within RBI tiered ceilings (85% / 80% / 75%); portfolio-weighted LTV not exceeding 75%; bullet tenure ≤ 12 months
Unsecured SME portfolio	Not more than 50% of AUM; single-borrower ceiling ₹25 lakh; surrogate-assessed loans not more than 40% of SME book
Non-Income-Proof portfolio	Not more than 10% of AUM; ticket size ₹10,000 to ₹1 lakh; tenure 3 to 24 months; dual sign-off above ₹50,000
Aggregate unsecured (SME + NIP)	Not more than 65% of AUM
Geographic concentration	No single state above 60% of AUM other than Odisha; no single district / branch cluster above 30% of AUM
Gross NPA trigger	Product-wise GNPA above 3% (secured) or 5% (unsecured) triggers RMC and origination review
Liquidity	Cumulative negative mismatch in the 1–30 day bucket ≤ 10% of cumulative outflows; liquidity buffer ≥ [5] months of debt service and operating outflows
Funding concentration	No single lender above 25% of total borrowings
Interest-rate sensitivity	Earnings-at-risk for a 100 bps shift not exceeding 10% of projected annual net interest income
Gold-price stress trigger	A 15% fall in gold price shall not push more than 7.5% of the gold book above 100% LTV; a 10% movement within 30 days triggers an RMC meeting
Operational & fraud loss	Aggregate operational and fraud losses not exceeding 2% of net worth in any financial year