KYC, AML & Fraud Risk Management Policy

R2P Capital Private Limited (the "Company") – *NBFC-ICC (Base Layer)*

1. Introduction & Objective

This consolidated policy sets out the Company's framework for **Know Your Customer (KYC)**, **Anti-Money Laundering (AML)**, and **Fraud Risk Management**, in compliance with:

- **RBI (NBFC – KYC) Directions, 2025**, and
- **Prevention of Money Laundering Act, 2002 (PMLA)** (and Rules thereunder, as amended).

The objective is to prevent the Company from being used for money laundering, terrorist financing, or other illicit activities, and to protect against fraud. This policy outlines mandatory requirements prescribed by RBI and PMLA, and also incorporates additional best-practice safeguards where appropriate. It applies to all customers (with a focus on corporate borrowers) and all employees of the Company. The policy will be reviewed periodically and updated for regulatory changes or emerging risks. The tone of this document is compliant, professional, and intended for review by the Company's Board and regulators.

2. Regulatory Framework

- **RBI KYC Master Direction (2025):** The Company shall adhere to RBI's Master Direction on KYC for NBFCs. This includes the four key elements of KYC compliance: **Customer Acceptance Policy, Risk Management, Customer Identification Procedures, and Monitoring of Transactions**.
- **PMLA and Rules:** The Company is a reporting entity under PMLA, 2002. It shall follow all customer due diligence, record-keeping, and reporting obligations as defined in the PMLA and the **Prevention of Money-Laundering (Maintenance of Records) Rules, 2005**.
- **FATF Standards:** The policy is in line with international best practices (e.g. FATF Recommendations) to maintain integrity of the financial system.
- **Scope:** This policy covers all products and services of the Company. It covers onboarding of customers (primarily companies and other legal entities), ongoing account monitoring, and measures to prevent, detect, and report fraud and money laundering.

3. Customer Acceptance Policy (CAP)

The Company shall formulate and implement a Board-approved **Customer Acceptance Policy** that lays down transparent criteria for accepting clients. Key principles of the CAP include:

- **No Anonymous or Fictitious Accounts:** The Company will not open or maintain any account under a false, fictitious, or "benami" name. Proper identification of the customer is a must.
- **CDD must be Completed:** No account will be opened **if the Company is unable to apply appropriate Customer Due Diligence (CDD)** measures. This may occur due to non-cooperation by the customer or if the information/documentation provided is insufficient or not reliable. In such cases, the Company will refuse the relationship and may consider filing a Suspicious Transaction Report (STR) to FIU-IND.
- **No Shortcuts on KYC:** The Company shall not undertake any transaction or establish an account-based relationship without completing the KYC/CDD process as required. All

mandatory information for KYC (such as identity details, address, PAN, etc.) must be obtained at onboarding and during periodic updates.

- **Specify Required Information:** The policy will clearly specify what minimum information and documents are required from customers for KYC at onboarding and for periodic KYC updates. Any additional information (beyond regulatory requirements) will be sought only with the customer's explicit consent.
- **Unique Customer Identification:** The Company shall apply CDD measures at the **Unique Customer Identification Code (UCIC)** level. This means if an existing customer (already KYC-compliant) wants to open another account or take a new loan, repetitive KYC is not required – their previous identification can be used.
- **Joint Accounts and Authorised Representatives:** For joint accounts or accounts where a person acts on behalf of another (e.g. an authorized signatory or power of attorney holder), the Company will perform CDD on **all relevant individuals** (all joint holders and the persons acting on others' behalf).
- **Sanctions List Screening:** No customer is accepted if they appear on any **sanctions lists** (such as UN Security Council lists or domestic lists for terrorists or banned organizations). Prior to onboarding (and regularly thereafter), the Company will screen customer names (including beneficial owners) against applicable sanctions/watch-lists. If a match is found with a designated individual/entity, the Company will not open the account, or will freeze any existing account and report to the appropriate authority as required by law (UAPA/UN sanction compliance).
- **PAN and Other Verifications:** Where Permanent Account Number (PAN) is obtained, the Company will verify the PAN with the issuing authority (Income Tax database). Likewise, if the customer provides a **digital signature** or **GST number**, the Company will verify the digital signature's validity and the GST number on the government portal.
- **Aadhaar Usage:** The Company shall not insist on Aadhaar for KYC; customers may voluntarily provide Aadhaar as an Officially Valid Document (OVD) at their discretion. (If a customer seeks a government subsidy benefit through our services, Aadhaar would be required as per Section 7 of the Aadhaar Act, otherwise any OVD can suffice.) When Aadhaar is used, the Company will comply with the Aadhaar Act provisions on authentication and privacy.
- **Financial Inclusion – No Unfair Rejection:** The Customer Acceptance Policy will not result in denial of financial services to members of the general public, especially those who are financially or socially disadvantaged. The Company shall not arbitrarily reject a customer's application for onboarding or KYC update without proper reasoning. Any rejection of an application will be based on risk considerations or inability to complete CDD, and the reason will be recorded by the officer with due care.
- **Suspicious Cases & Tipping-off:** If at any stage the Company suspects that a prospective customer is involved in money laundering/terrorist financing and **believes that performing CDD may tip off the customer**, the Company will **not proceed with further KYC** on that customer and will immediately file an STR with FIU-IND. Staff are trained that tipping off the customer about a pending STR is prohibited by law.

4. Customer Identification & Due Diligence (CDD)

Under PMLA and RBI directions, the Company must identify and verify the identity of every customer. The **Customer Due Diligence (CDD)** procedure involves obtaining documents to establish the identity and address of customers, and where applicable, the identity of those who own or control them (beneficial owners). The extent of CDD may vary according to risk category (see Section 5), but at a minimum the following standards shall apply:

- **Individuals:** For individual customers (if any), at least one **Officially Valid Document (OVD)** for proof of identity and address will be obtained and verified. OVDs include: Passport, Driving License, Voter's ID card, Proof of possession of Aadhaar (masking the Aadhaar number), NREGA job card, or any other document as notified by the government. A recent photograph and PAN (or Form 60 where PAN is not available) will also be obtained. The Company will verify the authenticity of these documents (e.g. Aadhaar verification through QR code/offline KYC, PAN through database, etc.). If an individual customer is a sole-proprietor or represents a business, additional documentation about the business may be collected as needed.
- **Businesses and Legal Entities:** For customers that are **legal entities** (companies, partnerships, trusts, etc.), the Company shall obtain a set of documents to identify the entity and its authorized officials, and to verify the **Beneficial Owners (BO)** behind the entity. Specifically:
    - **Companies (Corporate Customers):** Obtain certified copies of: (1) Certificate of Incorporation of the company; (2) Memorandum & Articles of Association; (3) the company's PAN card; (4) a Board Resolution (or letter of authority) authorizing the borrowing and specifying persons (directors/officers) who can transact on behalf of the company; (5) identification documents (as per individual KYC norms) for the authorized signatories, key managers, and **Beneficial Owners**; (6) the names and titles of current senior management and directors; and (7) the registered office and principal place of business addresses.
    - **Partnership Firms:** Obtain: (1) Registration certificate of the firm (if registered partnership); (2) Partnership Deed; (3) PAN of the partnership firm; (4) identity documents of the authorized signatory/partners, and of **Beneficial Owners** holding more than 10% interest (see definition below); (5) names of all partners; and (6) addresses of the partnership's principal place of business and registered office.
    - **Trusts:** Obtain: (1) Registration certificate of the trust; (2) Trust Deed; (3) PAN of the trust; (4) identity documents of the authorized signatories and **Beneficial Owners** (such as trustees, settlor, beneficiaries with ≥10% interest, any person with ultimate control); (5) names of the settlor, trustees, beneficiaries, and signatories; and (6) addresses of the trust's registered office/location. For trusts, all persons exercising effective control or having a significant interest (10% or more in the trust assets or income) are considered beneficial owners and must be identified.
    - **Unincorporated Associations/Societies:** Obtain: (1) Resolution of the managing body of the association/society authorizing the account and person to act on its behalf; (2) PAN or Form 60 of the unincorporated association/society; (3) identity details of the person holding the power of attorney to act on behalf of the entity; (4) identity documents of **Beneficial Owners** (natural persons owning ≥15% of the property or capital/profits, or controlling the management); and (5) any document to establish the legal existence of such an association or society (e.g. bye-laws, registration certificate).

(Unregistered partnerships and trusts are treated as "unincorporated associations" for KYC purposes.)

- **Other Legal Persons:** For any juridical person not covered above (e.g. government bodies, universities, local authorities), the Company will collect documents to verify the entity's legal existence and the authority of the person acting on its behalf, along with identification of relevant beneficial owners or controllers, as far as applicable.

- **Identification of Beneficial Owner (BO):** For non-individual customers, it is the Company's obligation to identify the **Beneficial Owners** – i.e., the natural person(s) who ultimately own or control the customer. As per RBI KYC Directions and PMLA rules, the thresholds for determining beneficial ownership are: **more than 10%** ownership or controlling interest in a company or partnership; more than 15% in an unincorporated association or body of individuals; or for trusts, all trustees, the settlor, and beneficiaries with ≥10% interest are treated as BOs. If no natural person meets the specified thresholds (for instance, in a widely-held company), the **senior managing official** of the entity shall be deemed the beneficial owner for CDD purposes. The Company will take all reasonable steps to verify the identity of the BOs using reliable, independent sources. BO identification and verification will be done at the time of onboarding a legal entity and also during periodic reviews.

- **Verification of Documents:** All KYC documents obtained will be verified for authenticity. Physical copies will be compared with the originals by an authorized officer (or verified digital signatures/e-documents as applicable). A **"certified true copy"** of an OVD or other KYC document means the Company's officer has seen the original and recorded this on the copy. For non-resident customers (e.g. NRIs/foreign companies), duly notarized or apostilled documents from acceptable officials (notary, magistrate, embassy, etc.) may be obtained as needed. Digital KYC processes (including Aadhaar offline verification, CKYC, or Video Customer Identification (V-CIP)) may be used as per RBI norms to facilitate customer identification in a secure manner.

- **Purpose and Business Profile:** As part of CDD, the Company will also collect information on the **nature of the customer's business, the purpose of the loan or account**, and expected usage patterns. Especially for corporate borrowers, understanding the customer's business model, source of funds/repayment, and the purpose of the loan facility is essential to establish a risk profile. This forms a baseline to detect any deviations or suspicious activities later.

- **Reliance on Third-Party KYC:** In general, the Company will perform its own due diligence. However, if allowed by RBI norms, it may **rely on third-party due diligence** (for example, if a regulated third-party intermediary has already completed KYC on a customer, and shares the KYC info as per rules). Such reliance will be in compliance with RBI conditions – e.g., the third party is regulated, follows equivalent KYC standards, and the ultimate responsibility remains with the Company.

- **High-Risk Case – Non-face-to-face Customers:** Given the Company's business (corporate loans), most customers interact directly. If ever the Company onboards a customer **without face-to-face interaction** (e.g. digital onboarding), it will apply enhanced measures: such accounts shall be classified as high-risk, the first funding transaction must originate from a KYC-compliant bank account in the customer's name, and enhanced monitoring will continue until a face-to-face verification or equivalent video-KYC is completed.

- **Refusal of Account Opening:** If a prospective customer refuses to provide KYC documents or information as required, or if the Company cannot verify the identity or intent of the customer to its satisfaction, the Company will **not open the account or disburse the loan**. In case an account has been opened but later information is found to be false or due diligence cannot be completed, the Company may freeze or close the account after issuing due notice, in line with regulatory guidelines. Any such instances will be evaluated for filing an STR as well.

5. Risk Categorization and Risk Management

The Company shall adopt a **Risk-Based Approach (RBA)** to AML, as required by RBI. Not all customers and transactions carry the same risk; therefore, the intensity of due diligence and monitoring will be commensurate with the risk profile of the customer. Key elements of our risk management approach:

- **Risk Category Definition:** Customers will be broadly categorized into **low, medium, or high risk** categories, based on the Company's assessment of their ML/TF risk. Risk categorization criteria will be approved by the Board. Generally:
    - *Low Risk:* Customers who are low-value and with well-defined identities and sources of funds. For example, government-owned companies, customers with conservative transaction profiles, etc.
    - *Medium Risk:* Customers that do not fit either low or high risk – for instance, moderately sized businesses with somewhat higher transaction volumes or occasional international exposure.
    - *High Risk:* Customers with greater likelihood of involvement in illicit activities or those for whom the consequences of something going wrong are severe. This includes customers with complex ownership structures, those in high-risk industries, non-resident or offshore entities, politically exposed persons, cash-intensive businesses, customers from high-risk jurisdictions, etc. By default, any account that is opened without face-to-face contact or through non-traditional methods will be treated as high risk until proven otherwise.
- **Risk Assessment Factors:** The Company shall consider various parameters when assessing a customer's risk level. Factors include:
    - **Customer Identity & Background:** Whether the customer is an individual or legal entity, public or private company, regulated entity or not, charitable organization or trust (NGOs can be higher risk due to possibility of misuse of funds), etc. For individuals, factors like occupation, public profile, or being a Politically Exposed Person (PEP) matter.
    - **Social/Financial Status:** The customer's income, financial standing, and credit history. Unusual wealth compared to known profile could raise risk.
    - **Nature of Business Activity:** The industry and business model of the customer. Certain lines of business are more prone to money laundering (e.g. casinos, real estate dealing, money changers, dealers in high-value goods, arms/explosives, etc.). In our context, if a corporate borrower operates in a sector with higher corruption or fraud incidence, they may be higher risk.

- **Location & Geographical Risk:** The country or region of the customer's operations. Customers based in countries with inadequate AML standards, or in regions known for trafficking, terrorism, or sanctions, are high risk. Domestically, certain areas with higher insurgency or crime rates may also elevate risk. Additionally, if the business has significant cross-border transactions, that adds risk.
- **Products/Services Used:** The type of loan or service availed. Our Company primarily offers corporate loans (term loans, working capital loans). These typically involve large amounts and thus require scrutiny. Products like accounts with frequent cash transactions, if any, would carry higher risk. (The Company currently does not offer deposit accounts; if it did, accounts with international wire transfers or remittances would get more attention.)
- **Transaction & Delivery Channel:** The manner in which services are delivered. Face-to-face dealings are lower risk than online-only relationships. Likewise, payments coming through banking channels are safer than cash. Use of third-party agents or intermediaries might add risk if not properly vetted.
- **Transaction Behaviour:** Expected vs. actual transaction volume and pattern. A customer whose activity consistently deviates from what's expected for their profile may be considered higher risk.

- **Confidentiality of Risk Classification:** The risk classification assigned to a customer and the rationale for it will be kept strictly confidential within the Company. Staff must not reveal to the customer whether they are categorized as high or low risk, or the specific risk indicators observed, so as to avoid "tipping off" any malicious actors. The Company will collect necessary information for risk assessment in a non-intrusive way and use it internally to determine the level of due diligence and monitoring required. (For example, we may ask additional questions or require more documentation for higher-risk customers, but we will not disclose that these actions are due to a risk rating.)
- **Use of Risk Information:** The categorization will influence how we manage the account: High-risk customers will be subject to **Enhanced Due Diligence (EDD)** measures (see Section 7) and more frequent monitoring, while low-risk customers may undergo simplified or less frequent reviews as allowed by RBI.
- **Periodic Risk Review:** The Company shall have a system to periodically review and, if needed, **update the risk categorization** of each customer. Risk profiles can change (e.g., a customer's business expands into new countries or a previously low-risk customer starts doing large transactions). At minimum, a risk re-assessment of each active account will be done **at least once every six months**. High-risk accounts may be reviewed more frequently. The review will consider any new information, changes in customer profile, changes in product usage, or external adverse news about the customer.
- **Group-wide Risk Assessment:** Since the Company is part of R2P Group, a consolidated risk view may be taken. As required by RBI, the Company will periodically conduct an enterprise-wide **Money Laundering/Terrorist Financing (ML/TF) Risk Assessment**, documenting the overall risks faced by the Company and the controls in place. This includes assessing risks across all products, delivery channels, customer types, and geographies. The Board or Risk

Management Committee will review this assessment and ensure that adequate mitigating controls are implemented across the organization.

- **Guidance and External Sources:** In assessing risk, the Company may refer to external guidance such as the FATF public statements on high-risk jurisdictions, typologies published by regulators or the **Indian Banks' Association (IBA)**, etc., to stay updated on current risk trends. Alerts or advisories from FIU-IND or RBI (for example, red flags for certain frauds or laundering methods) will be incorporated into our risk management procedures.

6. Ongoing Monitoring of Accounts

KYC is not a one-time exercise. The Company will conduct ongoing monitoring of customer accounts and transactions to ensure they are consistent with the customer's stated profile and risk level. This helps in detecting suspicious activities or anomalies that might indicate money laundering or fraud. Key aspects of ongoing monitoring:

- **Transaction Monitoring:** All transactions in the account will be monitored, especially large or complex transactions and patterns that do not fit the customer's profile. The Company will pay special attention to:
    - Transactions that are **large in amount or volume**, or **unusually complex**, given the nature of the customer's business. For example, a sudden one-time transfer or series of high-value payments that have no clear business rationale.
    - Patterns that **deviate from expected activity**. E.g., a corporate borrower whose loan proceeds are meant for domestic business suddenly transfers a significant sum abroad without obvious reason (this would be inconsistent and raise a flag).
    - Transactions that **exceed certain thresholds** set for specific categories. (For instance, if RBI or the Company sets triggers like cash transactions above a limit, etc., those will be flagged).
    - **High turnover with low balances:** Accounts where money comes in and goes out rapidly, with little maintained balance, could indicate layering of funds.
    - **Third-party payments:** Frequent deposit of cheques or funds from third parties followed by immediate withdrawals or transfers, which is not consistent with the stated purpose of the loan or account. For example, if a corporate loan account receives payments from entities unrelated to the borrower and then the funds are quickly withdrawn in cash or moved elsewhere, it may indicate the account is being misused to route funds.
- **Risk-Based Intensity:** The extent of monitoring will be aligned with the customer's risk category. High-risk accounts will be subjected to **more intensive and frequent monitoring**. This could include more frequent scrutiny of transactions, daily flagging of exceptions, and quarterly enhanced reviews. Low-risk accounts will still be monitored, but with a less aggressive lens (maybe automated alerts for major issues).
- **Periodic Reviews and KYC Updates:** The Company will perform **periodic KYC refresh** or re-verification of customer information. As per RBI norms, KYC information (documents, proofs) must be updated at least **every 2 years for high-risk, 8 years for low-risk, and 5 years for medium-risk customers** (or at such intervals as prescribed) – this ensures documents

remain current. In our policy, due to focus on corporate customers, we may opt to update KYC of all customers at least every 2-3 years or more frequently for high risk. During these updates, any change in ownership, management, address, or business of the customer should be obtained and verified. Significant changes trigger a re-assessment of risk.

- **Unusual Activity Handling:** If an account shows a **sudden change in activity pattern** (e.g., a dormant account becoming active with large transactions, or loan funds being utilized in an unintended manner), the compliance team will investigate the reason. The Company may contact the customer for clarification (without tipping off if it's potentially suspicious), and decide if these are justified by genuine business reasons or if they form grounds for suspicion.

- **Enhanced Monitoring Tools:** The Company may employ appropriate technology tools to aid in monitoring. This could include setting up rule-based alerts in the accounting/loan management system for transactions that meet certain risk criteria, and even exploring advanced tools like **Artificial Intelligence/Machine Learning** for pattern recognition in transactions. For example, machine learning models might help identify atypical transaction patterns that manual monitoring could miss. The Company will continuously improve its monitoring mechanisms as new tools and typologies emerge.

- **Specific Focus Areas:** Certain types of accounts or customers warrant extra caution. For instance, accounts of **marketing or multi-level marketing (MLM) companies** are known to be susceptible to pyramid scheme abuses – these will be closely watched for large scale money movements that could indicate a scam. If the Company has any client categorized as an NGO/NPO or dealing in high-cash businesses, those accounts will also have targeted monitoring.

- **Documentation of Findings:** All monitoring activities and decisions (e.g., why a particular alert was closed or why a transaction was deemed suspicious) will be documented. This ensures an audit trail for internal audit or regulatory inspection. If a STR is filed, the records of the investigation and rationale will be kept confidentially.

- **Account Closure or Freezing:** In cases where ongoing monitoring discovers serious KYC deficiencies or misuse of the account, the Company may decide to close the account or freeze transactions. This step will be taken in consultation with senior management and after considering the risk of tipping off. Any account closure due to suspicious activity will also be accompanied by an STR filing as applicable.

7. Enhanced Due Diligence (EDD)

Certain situations call for higher standards of due diligence beyond the regular KYC norms. The Company will apply **Enhanced Due Diligence** measures for customers or scenarios that are considered high-risk. EDD measures may include obtaining additional information, senior management approvals, increased monitoring, and any other measures to mitigate risk. Key cases requiring EDD are:

- **Politically Exposed Persons (PEPs):** PEPs are individuals who are or have been entrusted with prominent public functions (for example, foreign government officials, senior politicians, senior military officers, judiciary or state enterprise executives, important political party officials, etc.). Business relationships with PEPs (including their immediate family and close associates) are considered high risk. The Company may at its discretion choose whether to onboard a PEP customer or not; if it does, the following additional steps are mandatory:

- Put in place robust risk management systems to **determine if a customer or beneficial owner is a PEP**. (This involves asking the customer at onboarding, screening their names against known PEP lists/databases, and keeping track if any existing customer later becomes a PEP due to a change in position.)
- **Senior Management Approval:** Obtain approval from senior management (e.g. the CEO or designated committee) before opening an account for a PEP. Similarly, if an existing customer is subsequently found to be or becomes a PEP, continuing the relationship must be approved by senior management.
- **Source of Wealth/Funds:** Take reasonable measures to establish the **source of the PEP's funds and wealth**. Given the higher corruption risk associated with PEPs, understanding how they acquired their wealth (salary, business income, inheritance, etc.) and ensuring the funds for transactions are from legitimate sources is crucial. This may involve asking for income proofs, bank statements, or public disclosures of assets (if available).
- **Enhanced Ongoing Monitoring:** Transactions in PEP accounts shall be subject to heightened scrutiny on an on-going basis. Unusually large transactions or any transaction to/from government accounts or foreign accounts would be reviewed in detail. The Company will also refresh KYC of PEPs more frequently.
- Extend these measures to **family members and close associates** of PEPs as well, as they might be used as proxies. For example, if the spouse or child of a prominent politician is a customer, similar EDD applies.

- **Accounts from High-Risk Countries or Industries:** If the Company deals with customers from countries identified by FATF or RBI as having weak AML/CFT regimes (or subject to sanctions), those relationships will require EDD. This could include obtaining information on why the customer needs our services given jurisdiction differences, performing reference checks, and conducting more frequent reviews. Similarly, clients in industries like gambling, money service businesses, or crypto-assets (if any in future) would get EDD. (At present, the Company's focus is corporate loans to standard industries, but this policy notes the approach if high-risk industries are served.)
- **Non Face-to-Face / Digital Onboarding:** As noted earlier, customers who are onboarded without meeting in person will initially be treated as high risk. Until their identity is verified through a face-to-face interaction or equivalent strong digital process, such accounts will be under EDD. Enhanced monitoring (e.g. first transaction must come from the customer's own bank account) will apply. Additional verification via independent sources may be done (for instance, verifying the customer's business existence through site visits or reliable databases).
- **Large Exposure or Unusual Terms:** If a single customer or group of customers is asking for an unusually large loan or has an extremely complex deal structure, the Company will perform enhanced checks. This can include more detailed background checks (e.g. getting credit reports, reference from their bank, etc.), validating the genuineness of any collateral offered, and possibly engaging external investigative agencies if needed to verify claims.
- **Others as per Risk:** Any customer classified internally as "High Risk" (per Section 5) will be subject to EDD. This means we might collect additional KYC information (such as references,

details of major buyers/suppliers for a business, etc.), do verification of negative news (media search), and require more frequent account monitoring.

All Enhanced Due Diligence measures taken shall be documented. Senior management and the compliance officer must be involved in the decision-making for EDD cases. EDD findings may affect how we structure the account (for example, setting lower transaction limits or requiring certain conditions before disbursement). EDD is an ongoing requirement – if new high-risk factors emerge during the course of business, the Company will escalate those accounts for EDD, even if they were not originally so classified.

8. Record Keeping

Proper record-keeping is a cornerstone of KYC/AML compliance. The Company shall maintain all records of customer identity and transactions in systematic manner, as required by PMLA and RBI Directions. The key policies on record-keeping are:

- **Transaction Records:** All transactional records (ledger entries, payment records, loan disbursement and repayment details, etc.) between the Company and the customer (both domestic and international transactions) will be maintained **for at least 5 years from the date of each transaction**. In practice, since corporate loans may have long tenures, transactions will be kept for 5 years from the end of the loan or transaction. These records will include details sufficient to reconstruct each transaction – e.g. date, amount, currency, parties involved, type and purpose of transaction.

- **KYC Documents:** The Company will preserve all documents obtained during identification (account opening forms, KYC documents like IDs, incorporation papers, photographs, etc.), as well as all account files and business correspondence with the customer, for **at least 5 years after the end of the business relationship**. "End of business relationship" means the loan account is closed/terminated. If a one-off transaction was conducted, then records will be kept 5 years from its execution.

- **Maintaining Updated Info:** Records pertaining to identification will also include any updated KYC information or changes obtained during periodic KYC reviews. The Company should be able to demonstrate what information was relied upon at the time of onboarding and how it was updated over time.

- **Form of Records:** Records may be kept in physical or electronic form. The Company will ensure a proper electronic archive for easy retrieval of data. A retrieval system will be in place so that any required information can be made available **swiftly to competent authorities** upon request. For instance, if FIU-IND or RBI or law enforcement asks for details of a particular account or transaction, the Company's system should retrieve it promptly.

- **Transaction Details to Record:** In line with Rule 3 of PMLA Rules, the records of transactions will contain all necessary details to permit reconstruction, such as: (i) nature of the transaction (e.g. loan disbursement, repayment, fee payment, etc.), (ii) amount and currency, (iii) date of transaction, and (iv) parties involved (e.g. names of sender/recipient; in the case of wire transfers, the ordering and beneficiary institution details, etc.).

- **Record of Reports Made:** The Company will maintain records of all reports filed to FIU-IND (e.g. STRs, CTRs) and correspondence related to them securely, but separate from day-to-day

operational records to maintain confidentiality. The fact that a STR was filed on an account should be protected from unauthorized disclosure.

- **Non-profit Organizations (NPO) Accounts:** If the Company has customers that are registered **Non-Profit Organizations**, it will ensure that details of such NPOs are registered on the government's **DARPAN portal** (NITI Aayog) as required. Records of the NPO's DARPAN registration will be maintained for 5 years after the relationship ends. (This is a regulatory requirement to improve transparency of charities.)
- **Retention in Case of Investigations:** If records are subject to an ongoing investigation or subpoena, they may be required to be kept beyond 5 years. The Company will not dispose of any records that are known to be under investigation or have been requested by an authority, until it is confirmed that the matter is closed.
- **Disposition of Records:** After the retention period, disposal of records (especially those containing personal data) will be done securely (shredding of physical documents, permanent deletion of electronic data) to prevent unauthorized access. However, in general, as an NBFC, maintaining longer history might be useful, so the Company may choose to retain certain records for longer than 5 years unless space or privacy concerns dictate otherwise.

All employees are responsible for ensuring that no required records are tampered with or destroyed prematurely. Internal audits will periodically check that record-keeping is as per policy.

9. Reporting Obligations to FIU-IND

As a financial institution, the Company has legal obligations to report certain transactions to the **Financial Intelligence Unit - India (FIU-IND)** under PMLA. The Principal Officer will be responsible for timely and accurate reporting of the following:

- **Suspicious Transaction Reports (STR):** Any transaction (or attempted transaction) that the Company suspects may be linked to proceeds of crime, money laundering, terrorist financing, or any other criminal activity must be reported to FIU-IND. This is irrespective of the transaction amount. An STR will be generated if we detect *"red flags"* such as: inconsistent customer behavior, attempts to avoid KYC, use of the account for purposes other than stated, sudden activity in a dormant account, structuring of transactions to evade reporting thresholds, or any known unlawful activity. The STR should contain details of the suspect transaction and the reasons for suspicion. **Timing:** The STR must be filed with FIU-IND **within 7 days** of the internal determination that a transaction is suspicious. The decision to file an STR will be taken by the Principal Officer in consultation with senior management (if needed) and with appropriate confidentiality. It is emphasized that the Company **and its staff should not disclose to the customer** that an STR is being filed (no tipping-off). Operations in the account should not be suspended simply because an STR has been filed; the account can continue to be operated normally unless instructed otherwise by authorities. However, the compliance team may intensify monitoring on such accounts.
- **Cash Transaction Reports (CTR):** While the Company's business (corporate loans) typically doesn't involve cash transactions, it is still required to report to FIU any cash transactions that exceed the prescribed threshold. Currently, **cash transactions worth ₹1,000,000 (10 lakh) or more in aggregate in a month**, or any individual cash transaction above that amount, must be reported. Also, a series of connected cash transactions each below the threshold but totalling above ₹10 lakh in a month must be reported. CTRs are generated on a monthly basis. **Timing:**

The CTR for a month should reach FIU-IND by the 15th of the following month. (As a policy, the Company discourages cash repayments or disbursements for loans, to minimize this risk.)

- **Cross-Border Wire Transfer Reports (CBWTR):** Any international funds transfer of value ₹5,000,000 (50 lakh) or above (either incoming or outgoing) will be reported. This includes identifying details of sender/receiver. Given our current focus, this might arise if a borrower repays a loan from an overseas account or if our disbursement goes to an overseas account of the customer (subject to permitted regulations). Reports are filed in prescribed format to FIU.
- **NPO Transaction Reports:** If the Company deals with any registered trusts or NPO clients where donations or credits above a certain threshold (currently ₹1,000,000) are received in their account, such transactions are to be reported by 15th of next month as well. (This is mandated to monitor funds to non-profits.)
- **Fraud Reporting vs STR:** It's worth noting that fraud incidents are separately reported to RBI (see Fraud Risk Management section), whereas STRs to FIU are about suspected laundering/terror finance. However, there can be overlap; a fraud could involve laundering, and in such cases both reports may be warranted. The Principal Officer will use judgment to ensure all legal reporting duties are fulfilled.
- **Format and Manner:** The Company will use the prescribed electronic formats (submitted through FIU's online portal) for CTR, STR, and other reports. The Principal Officer should ensure the latest **reporting format guidelines issued by FIU-IND** are followed. If the Company's transaction data systems are not fully automated, the Principal Officer will collate data from branches or departments and use FIU's provided utilities to prepare reports. All reports will be delivered securely to FIU without any unauthorized viewing.
- **Regulatory Reporting (Rule 3 & 7):** In summary, the Company shall furnish to the Director, FIU-IND, all information in respect of transactions specified under **Rule 3** of the PMLA (Maintenance of Records) Rules, in the manner and periodicity specified under **Rule 7**. These include the reports described above. Each delay or omission in reporting such transactions within the time limit is treated as a separate violation, so timely compliance is critical.
- **Confidentiality of Reports:** All reports (STRs especially) are confidential. The fact that a transaction is under scrutiny or has been reported should not be disclosed to the customer or any irrelevant party. This also extends internally – information about STRs is shared on a need-to-know basis (e.g., with regulators, internal auditors, or law enforcement if required). Breach of confidentiality can attract penalties. The Company will, however, share information with regulatory/competent authorities as required by law and cooperate with any investigations (this sharing is not considered a tipping off).
- **Regulatory Cooperation:** Beyond FIU, if RBI or any other regulatory authority requests information (for example, under Section 12 of PMLA or under RBI Act), the Company shall furnish the requested records promptly.
- **Nil Reporting:** If there are no cash or suspicious transactions to report in a period, the Company is not mandated to file nil returns for STR/CTR. However, as a good practice, internal records will reflect that transactions were reviewed and no reportable events were identified for that period.

The Principal Officer will keep the Board of Directors and Audit Committee informed about the volume and nature of reporting done to FIU-IND periodically (for instance, a quarterly compliance report indicating number of STRs/CTRs filed, if any). This will be done in a manner that does not compromise the confidentiality of individual STR subjects.

10. Governance Structure & Internal Controls

A sound governance structure is essential to ensure effective implementation of KYC/AML and fraud prevention policies. The Company will institute the following governance and internal control measures:

- **Board Oversight:** The Board of Directors has overall responsibility for compliance with KYC & AML norms. The Board approves this policy and will review it at least annually (or sooner if required by regulation or if significant changes occur). The Board and senior management are committed to creating a culture of compliance and will ensure that adequate resources are devoted to AML/CFT efforts (e.g. training, technology, staffing).

- **Designated Director (AML/CFT):** In line with PMLA requirements, the Board will nominate a **Designated Director** for AML/CFT compliance. This is a senior official (e.g. a whole-time Director or equivalent) who ensures overall compliance with PMLA and KYC obligations. For our Company, the Designated Director is Goutam Banerjee, Director, reachable at goutam.banerjee@r2pcapital.com. The details of the Designated Director are communicated to FIU-IND and RBI as required. The Designated Director is not the same individual as the Principal Officer as required.

- **Principal Officer (PO):** The Company shall appoint a senior management officer as the **Principal Officer** for KYC/AML. The Principal Officer is responsible for day-to-day compliance with AML provisions, including monitoring transactions and sharing/reporting information to FIU and other authorities. The Principal Officer will also act as a central reference point for AML implementation and will have independent access to all data related to KYC/AML. For our Company, the Principal Officer is Bhupesh Dhawan, Director, reachable at bhupesh.dhawan@r2pcapital.com. The details of the Principal Officer are also communicated to FIU-IND and RBI as required. The Principal Officer will furnish the necessary reports (STRs/CTRs/etc.) promptly and engage with FIU/RBI for any feedback.

- **Compliance Department:** The Company's compliance function (under which the Principal Officer operates) will maintain and update internal KYC/AML guidelines. It will conduct sample tests of transactions, verify adherence to KYC procedures, and escalate any issues to management. Compliance will also ensure that latest regulatory updates (RBI Master Directions, FIU notices, etc.) are reflected in the policy and procedures.

- **Employee Hiring (Know Your Employee):** The Company will implement controls to **screen new hires**, especially for sensitive positions. A thorough background check (educational, previous employment verification, reference check, criminal record check where necessary) will be done for employees being hired. An internal **"Know Your Employee" (KYE) policy** will ensure we hire persons with integrity. Employees with dubious background can pose operational or fraud risks, so this is vital. The HR department will verify character and antecedents of all new staff and record that verification.

- **Employee Training:** Ongoing training programs will be conducted so that all staff are aware of KYC, AML, and fraud-prevention procedures. The training content will be tailored according to roles:
    - Frontline/operational staff who interact with customers or process transactions will be trained to identify suspicious documents or behaviour, and to follow due diligence steps properly. They should be adept at handling customer queries on KYC and obtaining required information tactfully.
    - Compliance and risk staff will receive deeper training on regulatory requirements, monitoring techniques, and emerging typologies of ML/TF and fraud.
    - Senior Management and Directors will be briefed on their oversight responsibilities and the Company's risk profile.
      Training will be done at induction and at least annually for all employees, with updates whenever regulations change. Records of training sessions (dates, topics, attendees) will be maintained to evidence compliance.
- **Internal Audit and Testing:** The Company's internal audit function (or an appointed external auditor) will periodically evaluate the effectiveness of KYC/AML and fraud controls. Auditors will test samples of customer files for KYC compliance, review STR filing decisions, and evaluate whether risk classification and transaction monitoring are functioning as designed. Any deficiencies or recommendations will be reported to the Audit Committee and senior management for timely rectification.
- **Independent Testing:** In addition to internal audit, the Company may engage external experts or use regulatory feedback to strengthen controls. For example, if RBI conducts an inspection and provides observations on AML, those will be addressed promptly.
- **Dual Control and Segregation:** Operationally, the Company will maintain dual-control principles to prevent internal fraud. No single employee should have end-to-end control of a transaction. For instance, the loan approval, disbursement, and account reconciliation will be handled by different people so that no one person can siphon funds without detection. Key processes will require at least two sets of eyes (maker-checker system). This also extends to KYC – one staff may collect and verify documents, but another (supervisor or compliance) should approve the KYC completeness.
- **Information Technology Controls:** Access to customer data and account systems will be restricted based on role. Audit logs will be maintained to see which staff accessed or modified records. This deters unauthorized alterations (for example, an employee trying to tamper with risk ratings or transaction records). The IT system will also enforce certain checks (like not allowing account activation until KYC fields are filled).
- **Retention of Control in Outsourced Activities:** If any element of customer due diligence or transaction processing is outsourced to a third party (such as a fintech partner for digital onboarding, or an outsourcer for document verification), the Company will ensure that such third party is compliant with our KYC standards. Legally, the compliance responsibility remains with the Company. Appropriate clauses will be included in outsourcing agreements to ensure data confidentiality and compliance with RBI norms.

- **Compliance with Updated Guidelines:** The Company's senior management shall ensure that any new instructions, guidelines, or clarifications from RBI or FIU-IND are promptly implemented. A high-level committee or the Designated Director may oversee that the institution is up-to-date in its compliance approach.

The governance structure described ensures that there are clear roles (Board, Designated Director, Principal Officer, etc.) and a chain of accountability for AML and fraud risk management. By embedding internal controls and a culture of compliance, the Company aims to not only meet regulatory requirements but also protect itself from reputational and financial risks associated with money laundering and fraud.

11. Fraud Risk Management Policy

In addition to AML controls, the Company is committed to the **prevention, early detection, and effective management of fraud risk** in all its operations. This section constitutes the Company's **Fraud Risk Management (FRM) Policy**, aligned with RBI's guidance on fraud risk management for NBFCs and industry best practices. "Fraud" for the purpose of this policy includes deliberate acts of omission or commission by any party (customer, employee, third-party, etc.) to cheat, misappropriate assets, or cause wrongful gain to oneself and wrongful loss to the Company. This covers loan frauds, misrepresentation, identity theft, bribery and corruption, accounting fraud, cyber fraud, and any other unauthorized act resulting in loss.

11.1 Fraud Risk Governance and Oversight

- **Board and Policy:** The Board of Directors owns the overall responsibility for fraud risk oversight. The Board shall approve the Fraud Risk Management Policy and review it at least once every **three years** (or more frequently if needed). The policy outlines the approach to fraud prevention, detection, investigation, reporting, and remedial action. Senior management is tasked with implementing this policy and reporting material fraud incidents to the Board. A culture of zero-tolerance for fraud will be promoted from the top.
- **Roles and Responsibilities:** The policy designates specific roles for fraud risk management:
    - **Designated Director:** Designated Director will coordinate the fraud risk program, including risk assessments, monitoring of controls, and fraud investigations.
    - **Operational Management:** Department heads (e.g. Credit Head, Operations Head) are responsible for fraud prevention controls in their respective functions (such as due diligence in credit underwriting to avoid loan fraud, or segregation in finance to avoid accounting fraud).
    - **Employees:** Every staff member has the duty to adhere to controls and to report any suspected fraud or irregularity immediately through the proper channels.
- **Fraud Risk Committee:** In line with RBI guidelines, the Company will establish a dedicated committee to monitor and follow up on fraud cases. Being a Base Layer NBFC, the Company has the option to form a **Committee of Executives (CoE)** instead of a Board-only committee. The Company chooses to constitute a *Fraud Monitoring CoE* comprising at least three senior members: e.g. the CEO/Managing Director (as Chair), one Whole-Time Director (or equivalent), and the Head of Risk/Compliance. This CoE will perform the roles akin to a Special Committee for Monitoring and Follow-up of Frauds (SCMFF) as prescribed by RBI. The committee will meet at least quarterly to review all frauds (actual or attempted), progress of

investigations, loss incurred, recovery steps, and overall effectiveness of fraud controls. One member of this committee will be designated to specifically review whistleblower complaints related to fraud. In addition to executives, a summary of the committee's discussions will be reported to the Audit Committee of the Board for oversight. *(If at a future date the Company moves to a higher regulatory layer or as a best practice, the Board may convert this to a Board-level Special Committee including independent directors, in line with RBI norms.)*

- **Natural Justice in Fraud Classification:** The Company will ensure that before classifying any account or person as "fraudulent," a fair and transparent process is followed, adhering to principles of **natural justice**. This means: those suspected of fraud will be given a chance to be heard. Specifically, if a borrower's account is to be declared fraud: a **show-cause notice** detailing the allegations will be issued to them (and any associated parties) and a minimum of 21 days will be given for them to respond. The Company will consider the responses and evidence impartially, possibly via the Fraud Risk Committee or an enquiry panel, before finalizing the fraud classification. A reasoned order (decision) will be recorded and communicated to the concerned parties, explaining the facts and circumstances leading to the fraud decision. This process helps prevent arbitrariness and protects the rights of all parties, as mandated by regulatory directions following court rulings.

- **Disclosure and Reporting to Board:** The Company shall disclose any significant fraud incidents to its Board promptly. Additionally, as per RBI requirements, the aggregate amount of frauds reported during a financial year will be disclosed in the Company's financial statements (notes to accounts). This ensures transparency and that the Board remains informed of fraud losses and provisions.

- **Integration with Enterprise Risk Management:** Fraud risk is recognized as part of the Company's overall risk management framework. The CRO/Risk Management Department will incorporate fraud risk in the periodic risk assessments. High-risk areas for fraud will be identified and remedial plans put in place. (For example, if lending against certain types of collateral has seen fraud instances, that will be tagged as a high-risk area and more robust checks instituted.)

11.2 Fraud Prevention Measures

Preventing fraud before it occurs is the first line of defense. The Company will implement the following preventive controls and practices:

- **Comprehensive Due Diligence:** Strong customer due diligence (as detailed in the KYC sections of this policy) is a key fraud prevention tool. By verifying identities, ownership, and credentials of borrowers and associated parties (directors, guarantors), the Company reduces the risk of impersonation or lending to shell entities. Enhanced background checks will be done for large exposures or where red flags appear during onboarding (e.g., verifying the corporate borrower's financial statements authenticity, checking credit bureau reports, market reputation checks with suppliers/customers of the borrower).

- **Credit Appraisal Safeguards:** In its lending processes, the Company shall institute checks to detect **fraudulent documentation or misrepresentation**. This includes verifying the genuineness of submitted documents (financial statements, invoices, property titles, etc.) through independent sources or site visits. For example, visiting the borrower's place of business to confirm operations, using third-party verification services for income/GST returns,

and confirming property details from public records. The credit team should be vigilant for signs of **forged documents** (erasures, inconsistencies) and **false statements**. If any such sign is found, the matter should be escalated to the fraud risk manager for further probe before loan approval.

- **Collaterals and Title Document Audit:** In corporate loans secured by assets (e.g., property, machinery), the Company will thoroughly verify title and ownership. Moreover, as per RBI guidance, for all loans of **₹1 crore (10 million) and above**, the Company will conduct **periodic legal audits of title documents** and verify them until the loan is fully repaid. This measure helps in detecting any cases where fake title deeds might have been given or if the same property was pledged to multiple lenders. Legal audits will typically involve an independent legal expert reviewing the property files for authenticity and ensuring the security interest is properly created.

- **Segregation of Duties:** Internally, sensitive functions will be segregated among employees to reduce opportunities for internal fraud or collusion. For instance, the employee who processes disbursement should not be the same who sanctioned the loan; accounting entries and reconciliations are done by separate staff from those initiating transactions, etc. The maker-checker system will require two sets of approvals for critical transactions, ensuring oversight.

- **Access Control and Cybersecurity:** The Company will maintain strict control over access to its information systems. User privileges are assigned based on role, and critical actions (like creating a new loan account, or disbursing funds) are logged and reviewed. Multi-factor authentication, strong passwords, and regular password changes are enforced to prevent unauthorized system access. The IT team regularly updates software and security patches to protect against cyber-fraud (like hacking or malware attacks). All electronic data transfers of funds will have encryption and, where feasible, transaction monitoring triggers.

- **Vendor and Service Provider Management:** Many frauds can occur through third-party service providers (valuers, collection agents, tech vendors). The Company will perform due diligence on any third-party it engages. Contracts with such service providers will include clauses making them accountable for any negligence or willful misconduct contributing to a fraud. For example, if a property valuer gives a highly inflated valuation which later is found fraudulent, the contract should enable the Company to take action against that valuer. The Company will maintain an approved panel of vendors (for verification, legal opinions, valuation, etc.) and periodically review their performance. Any red flags in their work (like repeated inaccuracies) will lead to delisting.

- **Whistleblower Mechanism:** The Company shall maintain an effective Whistleblower (Vigil) Mechanism to enable employees, customers, and other stakeholders to report, in good faith, any concerns or suspicions relating to fraud, misconduct, or unethical behaviour. Such reports may be made through designated confidential channels (including email or telephone), without fear of retaliation. All whistleblower complaints shall be reviewed by an independent authority designated by the Company, and the identity of the whistleblower shall be kept confidential to the extent permitted by law. The Company shall ensure protection to genuine whistleblowers and promote a culture of transparency and ethical conduct.

- **Employee Frauds – Staff Accountability:** The Company will reinforce employee integrity through a **zero-tolerance policy** for fraud. Pre-employment checks (as noted in Governance) help avoid hiring high-risk staff. Additionally, certain best practices will be instituted such as

mandatory leave rotation for staff in sensitive positions (e.g., requiring employees handling critical transactions to take block leave annually, during which another staff performs their duties – this can unearth any hidden frauds). Staff in key roles may be rotated to different assignments periodically to prevent long-term collusion or cover-up. The Company will also sensitize employees about the personal consequences of fraud (termination, legal action, and industry blacklisting). If any fraud involves staff, a staff accountability investigation will be conducted promptly after detection, as per internal HR procedures and regulatory guidelines. For significant frauds, especially those ≥ ₹30 million (3 crores) or involving senior management, the investigation outcomes may be reviewed by an external advisor or reported to the regulators as needed (public sector guidelines, etc., though our Company is private).

- **Training for Fraud Awareness:** Beyond AML training, focused **fraud risk training** will be provided to employees. This includes informing them about common fraud schemes in lending (e.g. diversion of funds, fake invoicing for working capital loans, cybersecurity frauds like phishing, etc.) and how to detect and prevent them. Case studies of actual frauds in the NBFC/banking sector (with sanitised details) can be shared to illustrate red flags. Specific teams like credit appraisal, operations, and IT will get specialized training on their relevant fraud risks.

- **Early Warning Systems (EWS):** The Company will develop an **Early Warning Signals** framework as a proactive measure to identify accounts which show signs of stress or potential fraudulent intent. While RBI mandates a formal EWS primarily for larger NBFCs (Middle/Upper Layer), as a best practice our Company will also incorporate an EWS approach for corporate lending. This involves tracking certain indicators on loan accounts such as:

    - Sustained delay in submitting periodic financial information or stock statements (could imply problems or hiding something).
    - Auditors of the borrower resigning or giving adverse opinions.
    - Frequent change in ownership or key management of the borrowing company.
    - Unexplained diversion of funds (money drawn from loan account going to unrelated parties).
    - The borrower's group companies defaulting elsewhere or being named willful defaulters.
    - Significant drop in borrower's revenues or profit margins without clear reason.
    - Any reports of legal disputes, lawsuits or regulatory actions against the borrower. These and other such **early warning signals** will be listed out in an internal EWS policy. If an account triggers one or more EWS, it will be examined closely by the credit monitoring team. Accounts with serious EWS indicators may be labeled as **Red Flagged Accounts (RFA)** internally, which prompts a deeper investigation before things worsen. The Fraud Risk Committee will oversee the effectiveness of the EWS and ensure it is integrated with our loan monitoring process.

- **Fraud Risk Assessment:** Periodically (at least annually), the Company will conduct a fraud risk assessment of its operations. This means identifying which processes are most vulnerable to fraud (e.g., loan origination, cash handling if any, vendor payments, IT systems) and evaluating whether controls in those areas are adequate. The assessment might use

methodologies like scoring likelihood and impact of different fraud scenarios. Based on findings, additional controls may be implemented. For example, if assessment finds that the process of verifying borrower's bank statements is weak (and could allow borrower to provide fake statements), the Company might introduce mandatory independent confirmation (like having borrower's bank send statements directly).

11.3 Fraud Detection and Monitoring

Despite the best preventive measures, some fraud attempts may occur. Early detection is critical to minimize losses. The Company will employ the following detection mechanisms:

- **Transaction and Account Monitoring:** Just as we monitor for AML, we also monitor for signs of fraud in transactions. The finance and operations team, aided by IT systems, will watch for anomalies such as: sudden withdrawals or transfers from loan accounts that are not in line with loan purpose, inconsistent patterns of fund usage, or any activity that seems to misuse the loan facility. For instance, if a working capital loan is meant to pay suppliers, but we observe payments going to personal accounts of directors, that's a red flag. Our systems or reports will flag such deviations for review by the risk team.

- **Loan Performance Monitoring:** The credit monitoring function keeps track of repayments. If a borrower starts missing payments or requests frequent rollovers, we scrutinize the underlying cause. While it may simply be financial difficulty, it could also be a sign of fraudulent intent (e.g., borrower never intended to repay fully, or diverted funds). Monitoring will include requiring periodic stock and receivables statements for working capital loans and checking for genuineness (if those statements show phantom inventory or debtors, it could signal fraud).

- **Early Warning Review:** As part of the EWS framework mentioned, any account that triggers multiple EWS indicators will be escalated for thorough review. This may involve a special audit or forensic examination of the account. The Company will ensure that for large exposures, we leverage credit bureau alerts or RBI's central fraud registry (if accessible) to see if the borrower's connected entities have issues elsewhere.

- **Audit of Suspicious Accounts:** If there is any **suspicion of wrongdoing or fraud in a particular loan account**, the Company will promptly arrange for a detailed investigation/audit of that account. This could be done by an internal audit team with specialized skills or by appointing an external forensic auditor. The Fraud Risk Management Policy mandates a predetermined process for such audits, including criteria for when to engage external experts (for example, if fraud over a threshold amount, or involvement of sophisticated methods). The Company will also, where feasible, include clauses in loan agreements that **allow the Company to conduct an audit or inspection of the borrower's books and assets** in the event of suspected fraud. (Such a clause makes it contractually easier to investigate, as the borrower has agreed to provide information on demand.) The scope of the audit will be to confirm whether funds have been misutilized, assets are genuine, and to quantify the extent of any fraud. If the account is found fraudulent, the auditor's report will support further action.

- **Cross-Group Scrutiny:** In case a borrower's one account is identified as fraudulent, the Company will also scrutinize **other related accounts** (group companies or connected borrowers). RBI directions require that if an account is declared fraud, the lender should examine the accounts of other group companies with common promoters or directors. We will follow that: for example, if Company X's loan is fraud and its director Mr. Y is also a director

in Company Z which has a loan with us, we will review Company Z's account for any warning signs. This prevents perpetrators from simply shifting fraud from one entity to another.

- **Use of Technology/Data Analytics:** The Company aims to harness data analytics to detect fraud patterns. For instance, analyzing the bank statements of borrowers through automated tools might reveal transactions typical of fraud (like round-tripping of funds between related entities). Data from public sources (news, MCA filings, etc.) can be aggregated to alert us if a borrower's name appears in a legal case or if their financial ratios show window-dressing. As resources allow, investment in fraud detection software or services (for example, negative news screening, machine learning models to score fraud risk) will be considered.

- **Surprise Inspections:** For certain loans (especially where stock or receivables are collateral), the Company may conduct random **surprise inspections** or calls for information to ensure the borrower has not falsified reports. E.g., unannounced visits to the borrower's warehouse to verify inventory levels, or asking for interim financial statements randomly. While primarily a credit risk tool, this can also catch fraud (if the stock is missing, maybe the stock reports were fake).

- **Internal Controls Monitoring:** The Company will also monitor internal processes to detect internal or collusive fraud. For example, the Compliance/Audit team will generate exception reports (list of loans approved bypassing certain guidelines, or any write-off of fees/charges beyond a limit, etc.) to see if any employee is consistently involved in exceptions that could indicate misconduct. Reconciliation differences, cash shortages, or IT system irregularities will be promptly investigated.

- **Whistleblower Reports Handling:** Any fraud tip received (from whistleblower channel or even anonymous sources) will be taken seriously. The Fraud Risk Committee or a designated Ethics Officer will evaluate the credibility of the complaint. If sufficient, an investigation team will be assigned discreetly to verify the allegations. Whistleblower complaints often provide early clues that formal controls might miss, so they will form a key part of our detection mechanism. The outcomes of such investigations will be reported to senior management/Board with recommended actions.

- **Coordination with Banks/Consortium:** In case the Company participates in any consortium or multiple banking arrangement for a borrower, we will actively share information with other lenders about any warning signs. Conversely, if another lender issues a **Red Flag** report about a shared borrower, we will treat it as a serious matter and investigate the status of our exposure to that borrower. This cooperation helps in early detection of frauds that span multiple institutions.

- **Incident Response Team:** When a fraud is detected or strongly suspected, the Company will activate an internal incident response. This may involve legal advisors, IT security (if cyber fraud), HR (if staff involved), and the concerned business unit, under the leadership of the Principal Officer or Fraud Risk Manager. The objective is to immediately contain the situation (e.g., stop further disbursements, secure evidence, etc.) while maintaining confidentiality.

All detection and monitoring efforts will be regularly refined. The Fraud Risk Committee will analyze every fraud incident (post investigation) to identify any **control gaps** that allowed it and will ensure those gaps are filled to prevent future occurrence (this is part of "root cause analysis").

11.4 Response to Fraud Incidents and Reporting

When a fraud is confirmed (or there is sufficient reason to believe a fraud has occurred), the Company will initiate a swift and coordinated response to mitigate loss, investigate the matter, and fulfill all legal reporting requirements. Key steps include:

- **Immediate Containment:** The first priority is to limit the financial loss and prevent further fraud. For instance, if a loan disbursement is in process and fraud is detected, immediately halt further disbursement. If funds have gone out but can still be recovered or frozen (say, lying in an escrow or not yet utilized), take steps to freeze those funds. In case of an internal fraud, restrict the involved employee's system access and, if necessary, suspend them from sensitive duties pending investigation.

- **Investigation:** A formal **investigation** will be carried out for each fraud incident, proportional to its severity. The Company will use internal or external investigators as appropriate. The investigation should gather all evidence, identify how the fraud was perpetrated, and who is responsible. It will cover the modus operandi, amount involved, and weaknesses in control that were exploited. The investigating team will maintain strict confidentiality to avoid alerting any suspect prematurely. All employees are required to cooperate fully with fraud investigations.

- **Reporting to Regulators (RBI):** As an NBFC, the Company must report fraud incidents to the Reserve Bank of India. RBI's **Master Direction on Frauds** (2024) requires that all frauds be reported via the **Fraud Monitoring Return (FMR)** system on the RBI portal. **Timeline:** The Company will report a fraud to RBI within **14 days** of classifying the incident as fraud. This applies to frauds of all values (no threshold – even a small fraud is reported). The report will contain details like parties involved, amount, nature of fraud, how it was detected, and actions taken. In addition, certain types of incidents have special timelines: any cases of **attempted or successful theft, burglary, dacoity, or robbery** at the Company (e.g., physical break-in or robbery of office) will be reported to RBI's Fraud Monitoring cell within **7 days** of occurrence. Such acts, though not directly ML/TF, are required to be reported for the safety and insurance tracking. The Company will also submit quarterly updates to RBI on such cases until they are closed/resolved.

- **Reporting to Law Enforcement:** Fraud is a criminal offense, so the Company will file a complaint/FIR with law enforcement agencies promptly. As required, the Company will designate a **nodal officer** to liaise with police/CBI and file the report. Typically, frauds involving amounts below a certain threshold might be handled by local police, whereas very large or complex ones could be referred to specialized agencies. The nodal officer will ensure all evidence is provided to law enforcement. This should be done **immediately on detecting the fraud** (ideally within the same week) to increase chances of recovery and bring culprits to justice. The Company will pursue legal recourse against perpetrators (customers or employees) including criminal prosecution and civil action for recovery of losses.

- **Internal Reporting and Escalation:** Every fraud incident will be immediately escalated to the CEO/Managing Director and the Board (or at least the Audit Committee Chair) once discovered. Significant frauds (say above a set monetary threshold, or involving senior staff, or any that attract media attention) will trigger an emergency notification to the Board. Management will keep the Board informed of progress of the investigation and recovery efforts.

- **Staff Accountability and Disciplinary Action:** If an employee is found involved in a fraud (or to have facilitated it through gross negligence), the Company will undertake a **staff accountability examination**. This will be done quickly, ideally within a few weeks of

concluding the fraud investigation. HR in conjunction with a management committee will determine the level of complicity or negligence and decide appropriate action. Action can range from reprimand and training (for minor lapses) to termination and legal action (for willful fraud or collusion). As per vigilance guidelines, if the Company were government-owned (which it isn't, but in case of any public sector involvement), cases above ₹3 crore would need reference to relevant vigilance boards. In our context, the principle is: no level of staff is immune – even senior executives will be held accountable if found at fault. The findings of staff accountability reviews will also be shared with the Board or its committees.

- **Recovery of Losses:** The Company will actively seek to recover any financial losses due to fraud. This includes enforcing collateral (in case of loan fraud, proceed to call in securities or guarantees), making claims under insurance policies (the Company will maintain a Banker's Blanket Bond or appropriate insurance that covers fraud scenarios), and legal attachment of assets of the fraudsters. If a customer fraudulently obtained a loan, their loan will be immediately recalled (terminated) and all legal means for recovery pursued, including suits or debt recovery tribunal proceedings. For employee fraud, any dues (like provident fund, etc.) may be withheld and adjusted if legally permissible. The Company will also coordinate with other institutions if it's a syndicated fraud to share information helpful in recovery.

- **Communication and Media Management:** In the event a fraud becomes public or media-attracting, only authorized spokespeople (for example, the CEO or a designated communications officer) will communicate on behalf of the Company. The messaging will be cautious so as not to violate confidentiality or defamation laws, but will reassure stakeholders that necessary actions are being taken. Under no circumstances should any employee other than authorized persons speak about an incident externally.

- **Documentation:** All aspects of the fraud (from detection, investigation, to final resolution) will be documented in a fraud case file. This file is confidential but will be used for regulatory reporting, audit review, and learning purposes. RBI may require updates on larger frauds; the Company will ensure timely submission of follow-up reports (e.g., progress report on fraud investigation if not concluded within 6 months). Once a fraud case is legally closed (like court case over or amount recovered), the Company may file a closure report on the RBI portal as guided (especially for frauds below ₹2.5 million as per RBI where closure can be initiated after certain conditions) – but closure is done only after ensuring all investigative leads are exhausted or there is no further progress for long.

- **Debarment of Fraudsters:** As per RBI's new directives, any borrower (and related entities/persons) who have been **classified and reported as fraud** by the Company will be **debarred from raising further finance** from any RBI-regulated financial institution for a period of 5 years from the date of full settlement of the fraudulently obtained amount. The Company will also not entertain any new credit proposals from such persons during that period. Essentially, those names get 'blacklisted' across the banking/NBFC system for 5 years. Even after 5 years, caution will be exercised if dealing with them again. The Company will also communicate and coordinate with credit bureaus to tag such accounts appropriately, so that other lenders are warned.

- **Remedial Actions:** After each fraud case, management shall implement remedial measures to prevent recurrence. This could mean plugging control gaps (e.g., adding a verification step, tightening an approval authority, improving an IT firewall, etc.), or even policy changes. A post-mortem report, including root cause analysis and lessons learned, will be prepared by the Fraud

Risk Manager and presented to the Fraud Risk Committee and Board. For example, if a fraud happened because an employee shared login credentials, a remedial action might be enforcing stricter password policies and disciplinary rules on credential sharing.

- **Notifying Stakeholders:** Depending on the fraud, certain stakeholders might need notification. For instance, if customer data was compromised in a cyber fraud, affected customers might need to be informed to take protective action (this also is ethical and possibly required by privacy regulations). Similarly, if an employee is terminated for fraud, an appropriate communication within the company might be made as a deterrent example (without disclosing unnecessary details). All such communication will be carefully handled with legal input.

The Company acknowledges that prompt and robust action in response to fraud not only helps in recovery but also serves as a deterrent for future attempts, by signalling that the Company will pursue fraudsters relentlessly through all legal means.

11.5 Red Flag Indicators of Fraud

It is useful to enumerate some common **red flag indicators** that could point to potential fraud in our line of business (corporate lending). Employees are expected to be mindful of these signs during their work:

- **KYC Red Flags:** Customer reluctant to provide original identification documents, or submits documents that appear altered, photocopied (where originals are expected), or are difficult to verify. Inconsistencies in information (e.g. different signatures, mismatch in date of birth across documents) may indicate identity fraud or impersonation.

- **Corporate Structure Red Flags:** Complex or opaque ownership structure of a borrower without a clear rationale (layering of shell companies, frequent changes in shareholding just before loan application) could be an attempt to conceal true beneficiary or past defaults. Similarly, if the company is recently incorporated with large capital but little operating history, and suddenly seeks a big loan, caution is warranted.

- **Financial Red Flags:** Borrower's financial statements show sudden and dramatic growth or unusual patterns that can't be explained, or many round figures. Auditors' qualifications or notes about inventory, debtors etc., in the financial report might hint something's off. Also, if revenues are increasing but cash flows are not (or vice versa), it might signal fictitious sales or siphoning.

- **Collateral Red Flags:** Proposed collateral is hard to value (e.g., specialized equipment with no secondary market), or located in a distant area making verification tough. Title documents that have corrections, or if the customer is strangely insistent on using a particular lawyer/valuer, it could be a collusion attempt. Also, pledging the same asset to multiple lenders is a known fraud – if a title search reveals prior charges not disclosed by the borrower, it's a red flag.

- **Usage of Funds Red Flags:** Once a loan is disbursed, monitor its usage. Red flag if funds are quickly diverted to personal accounts of promoters or unrelated businesses, rather than used for stated purpose. For example, a loan meant for purchase of machinery is disbursed to the supplier, but then the supplier immediately transfers money back to the borrower's related party – this circular flow suggests fraudulent diversion.

- **Repayment Behaviour Red Flags:** Borrower starts defaulting soon after loan disbursement, or pays one installment and then asks for refinancing or ever-greening. Early delinquency is

often a sign of fraud (they never intended genuine repayment). Also, if the borrower makes repayments but from accounts/name of third parties not in the loan agreement, it raises questions of layering or accommodation.

- **Communication Red Flags:** The borrower or their representative avoiding or delaying providing information, or being overly evasive when asked normal questions. If at the time of field visits or factory inspections, the borrower tries to prevent you from talking to certain staff or seeing certain areas, it may indicate they're hiding something (like non-existent inventory).
- **Employee Red Flags:** On the internal side, if an employee shows unusual closeness with a particular customer, or is seen bypassing procedure "to help" a customer, or living beyond known means, these could indicate bribery or collusion. Similarly, if critical reports or documents keep "getting lost" or delayed under a certain employee's watch, it could be intentional.
- **Third-Party Red Flags:** A valuer or lawyer in the panel whose valuations or opinions consistently seem too optimistic or favourable might be compromised. If one of our vendors (like a collection agent) is observed not following protocol or hiding information, it could be a sign they're involved improperly.
- **External Red Flags:** Negative news in media about the customer or its key people – e.g. allegations of fraud, involvement in legal cases, sudden resignations of top management, or their names appearing in defaulter lists or court orders – should prompt immediate review.

These indicators are not proof of fraud on their own, but they merit further scrutiny. Staff are expected to use judgment and escalate anything that "doesn't feel right" even if they can't fully pinpoint the issue. It is better to have false alarms investigated than to miss a real fraud. The Company will keep updating this red-flag list as new fraud patterns emerge in the industry.

11.6 Continuous Improvement and Review

The fraud risk landscape is evolving with new schemes and technologies. The Company will keep its fraud risk management practices current by:

- Reviewing this Fraud Risk Management Policy at least every three years (sooner if required), and after any major fraud incident to incorporate lessons learned.
- Staying updated with RBI circulars, industry reports, and law enforcement feedback on frauds. If RBI issues a caution notice on a certain modus operandi (for example, scams involving fake fixed deposit receipts as collateral which happened in banking industry), the Company will proactively guard against it.
- Participating in industry forums or fraud information-sharing networks (like the RBI's Central Fraud Registry or Credit Bureau fraud prevention services) to exchange data on fraudulent borrowers or trends.
- Ensuring our internal audit includes fraud risk management in its scope regularly and that their suggestions for improvement are implemented.

Conclusion: The Company affirms that strict adherence to this KYC, PMLA and Fraud Risk Management Policy is not only to satisfy regulatory compliance, but to uphold high standards of integrity and trust in our operations. All directors, officers, and employees are expected to understand their roles in this policy's implementation. Any wilful non-compliance or negligence in following these

norms will be taken seriously. By diligently applying the procedures laid out – from customer acceptance and due diligence to vigilant monitoring and decisive action on frauds – the Company aims to foster a secure and compliant financial environment for its customers, employees, and stakeholders.