

POLICY FOR PREVENTION OF MONEY LAUNDERING (PMLA) & ANTI-MONEY LAUNDERING (AML)

1. PURPOSE AND SCOPE

This Policy establishes the methodology to classify clients of BondNest Capital India Securities Private Limited, operating the MeraDhan online bond platform ("Company"), as **Low, Medium or High AML Risk**.

The classification represents the client's risk from an anti-money laundering, terrorist-financing and proliferation-financing perspective. It is separate from the client's investment risk profile or suitability assessment.

This Policy applies to:

- Individual and non-individual clients;
- Clients onboarded through online, offline, KRA, CKYCR or digital KYC processes;
- Beneficial owners, authorised signatories, trustees, partners, directors and controlling persons; and
- Existing as well as prospective clients.

The Company shall follow a risk-based approach and consider the client's identity, occupation or business, ownership structure, geography, source of funds, transaction behaviour, onboarding channel and adverse information before assigning a risk category.

2. RISK ASSESSMENT PRINCIPLES

Risk classification shall be completed before activation of the client's trading account or before permitting the first transaction.

The following principles shall apply:

1. The highest applicable risk factor shall prevail over the overall assessment.
2. A client shall not be classified as Low Risk merely because the KYC is validated by a KRA or CKYCR.
3. Simplified due diligence shall not be applied where there is any suspicion of money laundering, terrorist financing, identity misuse or source-of-funds mismatch.
4. Risk classification shall not be based solely on investment amount, income, profession, nationality or legal constitution.

5. The Company may assign a higher risk category based on its independent assessment, adverse information or unusual transaction activity.
6. All payments must be received from the client's verified bank account and securities must be credited to the client's verified demat account.

3. CLIENT RISK CATEGORIES

3.1 Low-Risk Clients

A client may be classified as Low Risk where the identity, source of funds, ownership and expected transaction activity are transparent and no material risk indicator is identified.

Low-Risk profiles may include:

- Resident Indian salaried employees, pensioners or professionals with a regular and identifiable source of income;
- Resident individuals investing amounts consistent with declared income, net worth and occupation;
- Government departments, statutory bodies, public-sector entities and listed companies with transparent ownership;
- Regulated financial institutions, subject to satisfactory verification;
- Clients with KRA-validated or CKYCR records, successfully verified bank and demat accounts and no material discrepancy;
- Clients completing face-to-face or permitted video-based identification; and
- Clients with no PEP, sanctions, adverse-media or suspicious-transaction indicators.

Controls: Standard KYC and transaction monitoring.

Risk review: At least once every three years, subject to applicable KYC-update requirements, and immediately upon occurrence of a trigger event.

3.2 Medium-Risk Clients

A client shall ordinarily be classified as Medium Risk where the profile is legitimate and verifiable but requires additional understanding or monitoring because of the nature of the client, business or expected transactions.

Medium-Risk profiles may include:

- Self-employed persons, proprietors or persons engaged in businesses with variable income;
- HUFs, partnership firms, LLPs and private limited companies having a clear and verifiable ownership structure;
- Closely held entities where beneficial ownership is established and no other high-risk indicator exists;
- Clients engaged in cash-intensive businesses, subject to satisfactory verification of income and source of funds;
- Clients whose investment amount is materially higher than their historical activity but is supported by documentary evidence;
- Clients having multiple bank or demat accounts with a reasonable explanation;
- Clients requiring manual resolution of non-material KYC, name, address or bank-account discrepancies; and
- Clients whose occupation, financial information or expected transaction volume requires additional verification.

Additional controls may include:

- Documentary evidence of income, net worth or source of funds;
- GST returns, audited financial statements, income-tax returns or bank statements;
- Beneficial ownership declaration and ownership chart;
- Verification of the purpose and expected level of investment; and
- Compliance review before account activation or execution of unusually large transactions.

Risk review: At least once every two years and immediately upon occurrence of a trigger event.

3.3 High-Risk Clients

Clients presenting elevated money-laundering, terrorist-financing, sanctions, ownership, geographic or reputational risk shall be classified as High Risk.

The following shall ordinarily be treated as High Risk or Clients of Special Category:

Non-resident clients;

- High-net-worth clients as determined under the Company's approved internal threshold;
- Trusts, charities, NGOs, non-profit organisations and organisations receiving donations;

- Politically Exposed Persons, their family members and close associates;
- Companies having close family shareholding or beneficial ownership;
- Clients connected with foreign-exchange or money-service activities;
- Clients resident in, operating from or materially connected to high-risk jurisdictions;
- Clients onboarded entirely on a non-face-to-face basis, other than permitted video-based identification;
- Clients having complex, layered, nominee or opaque ownership structures;
- Clients with adverse media, regulatory action, criminal allegations or a dubious reputation;
- Clients whose source of funds or wealth cannot be readily established;
- Clients displaying unusual transaction, payment, cancellation or refund patterns; and
- Any client classified as High Risk by the Principal Officer or Compliance Officer based on independent judgement.

SEBI identifies non-residents, HNIs, trusts, charities, NGOs, closely held entities, PEPs, clients connected with high-risk countries, non-face-to-face clients and persons with a dubious reputation as categories requiring enhanced due diligence.

Enhanced Due Diligence shall include, as applicable:

- Approval from the Principal Officer/Compliance Officer and senior management before onboarding or continuing the relationship;
- Verification of source of funds and, where appropriate, source of wealth;
- Additional identity and address verification;
- Detailed verification of business activity and beneficial ownership;
- PEP, sanctions, UAPA, UNSC and adverse-media screening;
- Review of expected annual investment and transaction pattern;
- Closer scrutiny of all payments, refunds and securities transfers; and
- Enhanced and more frequent transaction monitoring.

Risk review: At least annually and immediately upon occurrence of a trigger event.

4. MANDATORY REJECTION OR ESCALATION

The Company shall not open or continue an account where:

- The client is anonymous, fictitious or acting for an undisclosed person;
- The identity of the client, authorised person or beneficial owner cannot be verified;
- KYC documents appear forged, manipulated or unreliable;
- The client refuses to provide required information regarding ownership, source of funds or purpose of investment;
- A confirmed sanctions or designated-person match is identified;
- Payment is proposed from an unexplained third-party account;
- The Company cannot satisfactorily resolve a material PAN, bank, demat, address or ownership discrepancy; or
- Continuing the relationship would breach applicable law, SEBI directions, exchange requirements or sanctions obligations.

Such cases shall be immediately referred to the Principal Officer. The Principal Officer shall determine whether the account must be rejected, restricted, frozen or closed and whether a Suspicious Transaction Report or any other regulatory communication is required. No employee shall disclose to the client that an STR is being considered or filed.

5. TRANSACTION-MONITORING TRIGGERS

The client's risk category shall be reviewed when any of the following occurs:

- Sudden or unexplained increase in investment value or frequency;
- Transactions inconsistent with declared income, business or net worth;
- Repeated order cancellations, payment reversals or refund requests;
- Payment attempts from third-party or unregistered bank accounts;
- Requests to transfer securities to an unrelated demat account;
- Multiple clients using common contact, device, bank or demat information without reasonable explanation;
- Frequent changes to bank, demat, mobile number, email or beneficial ownership;
- Adverse media, PEP status, sanctions or regulatory action identified after onboarding;

- Unusual interest in transaction structuring, reporting thresholds or bypassing controls; or
- Any activity lacking an apparent economic or legitimate purpose.

SEBI requires intermediaries to understand the client's normal activity, identify deviations and examine complex or unusually large transactions and patterns lacking an apparent economic purpose.

6. RESPONSIBILITY AND RECORDS

The KYC/Operations team shall record the initial classification and supporting rationale. Medium- and High-Risk classifications shall be reviewed by Compliance.

The Principal Officer shall have authority to upgrade any client's classification, require additional documents, restrict transactions or recommend discontinuation of the relationship.

The Company shall retain the risk assessment, approvals, KYC documents, beneficial ownership records, transaction reviews and supporting correspondence in accordance with PMLA, SEBI and exchange-prescribed retention requirements. Client and transaction records are generally required to be retained for at least five years under the PMLA framework.

7. APPROVAL AUTHORITY & REVIEW OF POLICY

The policy is approved by the Board of BondNest Capital India Securities Private Limited. This policy may be reviewed as and when there are any changes introduced by any statutory authority or as and when it is found necessary to change the policy due to business needs post the approval of our Board of Directors.

8. POLICY COMMUNICATION

A copy of this policy shall be made available to all the relevant staff/persons such as: compliance officer / department in-charge /authorized persons.

In addition, a copy of this policy has also been added on our website.