

KYC AND AML POLICY

SelfFin India Financial Services Private Limited

Contents

1. Introduction
2. Scope and Application of the Policy
3. Customer Acceptance Policy
4. Guidelines for Accepting Customers – Due Diligence of Customers – Reliance on Third Party for Due Diligence of Customers
5. Officially Valid Document
6. Risk Level Categorization
7. Due Diligence of Business Partners
8. Due Diligence on Employees
9. Purposeful Implementation
10. Customer Identification Procedure (CIP)
11. Digital KYC Process
12. Provisions under PMLA
13. Monitoring of Transactions and Maintenance of Records of Transactions
14. Preservation of Records
15. Reporting to Financial Intelligence Unit-India (FIU-INDIA) – CTR, STR and CCR
16. Other Essential Aspects Related to CTR and STR Reporting
17. Monitoring & Reporting of Transactions
18. Risk Management
19. Updation / Periodic Updation of KYC
20. Compliance of KYC Policy
21. Policy Implementation Guidelines
22. Appointment of Principal Officer and Role of Principal Officer
23. Money Laundering and Terrorist Financing Risk Assessment and Monitoring of Risk – Adopting Risk Based Approach
24. Combating Financing of Terrorism
25. Countries which do not or insufficiently apply the FATF recommendations
26. Inter-Governmental Agreement (IGA) with United States of America (US) under Foreign Accounts Tax Compliance Act (FATCA) – Registration
27. Constitution of Special Investigating Team – Sharing of Information
- Annexure A – Indicative List for Risk Categorization

1. Introduction

The purpose of this KYC, Anti-Money Laundering and Combating the Financing of Terrorism framework is to ensure that SelfFin India Financial Services Private Limited ("SelfFin" or "the Company") is not used, knowingly or unknowingly, for money laundering, terrorist financing, fraud or other unlawful activities. The policy is designed to support appropriate customer identification, verification, monitoring and reporting while protecting the integrity and reputation of the financial system.

SelfFin shall implement this policy in accordance with the Prevention of Money Laundering Act, 2002 ("PMLA"), the Prevention of Money-laundering (Maintenance of Records) Rules, 2005 ("PML Rules"), the Reserve Bank of India's Master Direction – Know Your Customer (KYC) Direction, 2016, as amended from time to time, applicable RBI directions and circulars, and other applicable laws and regulatory requirements. The policy shall also take into account applicable standards relating to Anti-Money Laundering ("AML") and Combating Financing of Terrorism ("CFT").

The policy shall be read together with the Company's internal procedures, customer acceptance standards, risk-management framework and other applicable compliance policies. Where applicable law or a regulatory direction is amended, the amended requirement shall prevail to the extent of any inconsistency.

2. Scope and Application of the Policy

This policy is intended to establish a consistent framework for:

- setting appropriate criteria for accepting customers and establishing business relationships;
- identifying and verifying customers and beneficial owners;
- maintaining appropriate customer and transaction information;
- monitoring customer activity and identifying unusual or potentially suspicious transactions;
- reporting prescribed transactions and suspicious activity to the competent authorities; and
- supporting a risk-based approach to AML/CFT controls.

The key components of SelfFin's KYC/AML framework include:

- Customer Acceptance Policy
- Customer Identification Procedure
- Customer Due Diligence
- Risk Management and Transaction Monitoring

3. Customer Acceptance Policy

SelfFin shall maintain a customer acceptance framework designed to ensure that a business relationship is not established unless the Company can appropriately identify and verify the customer, understand the purpose and intended nature of the relationship and apply the required customer due diligence measures.

The Company shall not open an account or establish a customer relationship in circumstances where:

- the customer cannot be identified or verified in accordance with applicable KYC requirements;
- the information or documents required for customer identification are materially incomplete or unreliable and the deficiency cannot be satisfactorily resolved;
- the Company cannot determine the beneficial owner or the person acting on behalf of the customer, where such identification is required;

- the proposed relationship is inconsistent with the Company's customer acceptance standards or applicable law; or
- the relationship would expose SelfFin to an unacceptable legal, regulatory, reputational or money-laundering/terrorist-financing risk.

Customer acceptance criteria shall not be applied in a manner that unfairly excludes financially or socially disadvantaged persons. However, no customer shall be accepted where the Company is unable to complete the legally required KYC/CDD process.

Definition of Customer

For the purposes of this policy, a customer may include:

- a person or entity maintaining an account or business relationship with SelfFin;
- a person on whose behalf the account or relationship is maintained, including the beneficial owner where applicable;
- beneficiaries of transactions carried out through professional intermediaries, where relevant;
- trustees or other persons permitted to act under applicable law; and
- any other person or entity whose transaction or relationship with SelfFin requires customer identification under applicable law.

The term "person" shall be interpreted in accordance with applicable KYC/PMLA requirements and may include individuals, companies, firms, associations, trusts, government bodies and other legally recognised entities.

4. Guidelines for Accepting Customers – Due Diligence of Customers – Reliance on Third Party for Due Diligence of Customers

SelfFin shall observe the following principles while establishing and maintaining customer relationships:

- No anonymous or fictitious accounts shall be opened or maintained.
- No account or relationship shall be established where the Company is unable to complete appropriate customer due diligence because required documents or information cannot be obtained or verified.
- Customer acceptance shall be based on a clear understanding of the customer's identity, business/activity, ownership or control structure where applicable, and the purpose and expected nature of the relationship.
- KYC information shall be obtained and periodically refreshed in accordance with the customer's risk classification and applicable regulatory requirements.
- Information collected for KYC purposes shall be proportionate to the nature and risk of the relationship and shall be handled in accordance with applicable privacy and data-protection requirements.
- Where customer identification is performed by or through an eligible third party, SelfFin shall ensure that reliance is permitted under applicable law and that the required CDD information and records can be obtained without undue delay.

Due diligence by or through third parties shall not dilute SelfFin's ultimate responsibility for complying with applicable KYC/AML requirements. SelfFin shall ensure that the relevant third party is subject to appropriate KYC obligations and that records are accessible when required.

5. Officially Valid Document

For customer identification, SelfFin shall obtain and verify officially valid documents (“OVDs”) and other documents/information permitted under applicable RBI KYC requirements. An OVD generally includes a passport, driving licence, proof of possession of Aadhaar number, voter’s identity card, NREGA job card signed by an officer of the State Government, or a letter issued by the National Population Register containing details of name and address.

Where the customer submits a document or information in an alternative form permitted under applicable law, SelfFin shall apply the verification and record-keeping requirements applicable to that form of identification.

6. Risk Level Categorization

Customer risk classification is a core component of SelfFin’s risk-based KYC/AML framework. The Company shall assess the money-laundering, terrorist-financing, fraud and other relevant risks associated with a customer and apply controls proportionate to the level of risk.

Risk assessment may consider, among other factors:

- customer identity, ownership and control structure;
- nature of the customer’s business or occupation;
- geographical exposure and location of the customer and counterparties;
- source of funds and, where appropriate, source of wealth;
- products and services used;
- transaction behaviour, volume, frequency and complexity;
- delivery channels and use of intermediaries or non-face-to-face methods;
- whether the customer or related persons are politically exposed persons (PEPs);
- adverse media, sanctions, law-enforcement or other reliable risk information; and
- any other factor that may increase or reduce AML/CFT risk.

Customers shall ordinarily be classified into low, medium or high-risk categories, or such other categories as may be approved under SelfFin’s risk framework. The reasons supporting a customer’s risk classification shall be documented and treated as confidential.

Low Risk Customers

Low-risk customers may include individuals and entities whose identity and source of wealth/funds can be satisfactorily established and whose activities and transaction patterns do not present material AML/CFT concerns.

Medium / High Risk Customers

Higher-risk characteristics may include customers with complex or opaque ownership, PEP relationships, significant cash activity, exposure to higher-risk jurisdictions, unusual or complex transaction patterns, adverse information, non-face-to-face onboarding without adequate controls, or other indicators suggesting elevated AML/CFT risk. Higher-risk customers shall be subject to enhanced due diligence and monitoring. An indicative list of higher-risk categories is provided in Annexure A.

7. Due Diligence of Business Partners

Before onboarding a business partner, SelfFin shall perform due diligence appropriate to the nature and risk of the proposed relationship.

A. Verification of Identity

- obtain and verify applicable incorporation, registration and statutory documents;
- confirm the legal existence and ownership/control information of the entity;
- obtain appropriate licences or regulatory registrations where relevant to the business;
- obtain supporting information sufficient to establish the nature and legitimacy of the proposed relationship; and
- perform sanctions, adverse-media and other relevant screening where appropriate.

B. Verification of Source of Income / Financial Standing

- review publicly available or reliable commercial information concerning the business;
- assess the financial standing and nature of business activity relevant to the relationship; and
- maintain appropriate evidence of the due-diligence steps undertaken.

8. Due Diligence on Employees

SelfFin shall conduct proportionate due diligence on prospective employees before joining and, where appropriate, during employment, particularly for employees in sensitive or customer-facing roles.

A. Verify Identity

Identity and address documents shall be obtained and verified as appropriate. Depending on the role and applicable requirements, documents may include:

- passport
- PAN
- driving licence
- valid Aadhaar-related document or other permitted identity/address document
- voter identity card

B. Verify Domicile / Residence

An appropriate utility bill or other acceptable address-verification document may be obtained and checked against the address provided by the employee.

C. Verify Previous Employment Record

- Where relevant, SelfFin may contact the previous employer to validate employment history and credentials.
- The address and other information of the previous employer may also be verified where appropriate.

D. Check References

- SelfFin may obtain and verify professional references from the prospective employee.
- References may be confirmed with appropriate persons within the previous employer or other reliable sources.

Information collected for employee due diligence shall be treated as confidential and shall be used only for legitimate employment, risk-management and compliance purposes.

9. Purposeful Implementation

The purpose of the KYC/AML framework is to ensure that customers are accepted and serviced in a manner consistent with SelfFin's risk appetite and regulatory obligations. The Company shall not discriminate against customers based on legitimate financial or social circumstances; however, the Company may decline or restrict a relationship where required KYC information cannot be obtained or where the relationship presents an unacceptable risk.

SelfFin shall also ensure that products and services are not promoted or structured in a manner that knowingly facilitates circumvention of KYC/AML controls or encourages customers to transact beyond their legitimate financial capacity.

10. Customer Identification Procedure (CIP)

Customer Identification Procedure means the process of identifying and verifying the customer and, where applicable, the beneficial owner, authorised representative or person acting on behalf of the customer. SelfFin shall collect sufficient information to understand the identity and nature of the relationship and the documents/information required may vary depending on the customer category and risk.

Need for Photograph

- Where required under applicable KYC rules, a photograph or equivalent identity-verification image shall be obtained.
- Where a customer is represented by an authorised signatory, trustee or other representative, appropriate identification and authority documents shall also be obtained.

Proof of Customer Address

Where address verification is required, SelfFin may use documents such as:

- Aadhaar-related document
- Voter identity card
- Driving licence
- Passport
- Electricity/utility bill or other acceptable address proof

Customer identification shall be undertaken in appropriate circumstances, including:

- at the commencement of an account-based relationship;
- when there is a material doubt about the authenticity or adequacy of previously obtained identification data;
- when the customer's transaction pattern indicates a material change in the nature or risk of the relationship;
- when the Company has reason to believe that the account or relationship is being used for an unlawful or suspicious purpose;
- where cumulative or linked transactions exceed applicable regulatory thresholds or otherwise require enhanced verification; and
- where applicable law or internal risk controls require fresh or additional identification.

11. Digital KYC Process

Where Selfin uses a digital KYC process, the process shall comply with the applicable RBI KYC Directions and other legal requirements. The Company shall use secure, auditable and controlled digital methods for customer identification and verification.

- Digital KYC shall be performed through an approved application or platform and shall be accessible only to authorised personnel or authorised systems.
- Customer consent shall be obtained for the collection and processing of information as required.
- Where live photograph or video-based verification is required, the process shall capture the customer and relevant identification information in a manner that supports authenticity and auditability.
- Information entered into the customer application form shall be reconciled with the documents and verification information obtained during KYC.
- One-time passwords, digital signatures, electronic verification or other authentication mechanisms shall be used only in accordance with applicable regulatory requirements and approved procedures.
- Electronic records and audit trails shall be maintained so that the KYC process can be reconstructed when required.

12. Provisions under PMLA

Selfin shall comply with the obligations applicable to reporting entities under the Prevention of Money Laundering Act, 2002 and the Prevention of Money-laundering (Maintenance of Records) Rules, 2005, as amended from time to time.

At the commencement of a customer relationship and during its continuance, Selfin shall, as applicable:

- identify the customer and verify identity using reliable and independent sources;
- identify and take reasonable measures to verify the beneficial owner;
- understand the purpose and intended nature of the relationship;
- conduct ongoing due diligence and monitor transactions on a risk-sensitive basis;
- maintain and preserve prescribed records; and
- report transactions and information to the Financial Intelligence Unit–India (FIU-IND) or other competent authority in the prescribed manner and time.

13. Monitoring of Transactions and Maintenance of Records of Transactions

Ongoing transaction monitoring is an essential component of Selfin's KYC/AML programme. The Company shall maintain systems and controls that enable transactions to be reviewed against the customer's profile, expected activity, source of funds and risk classification.

Monitoring shall consider, among other things:

- large, unusual, complex or economically unexplained transactions;
- transactions inconsistent with the customer's stated business, occupation or financial profile;
- unusual cash activity or repeated cash transactions;
- transactions involving higher-risk jurisdictions or sanctioned persons/entities;
- rapid movement of funds or patterns suggesting layering, structuring or other suspicious activity;
- multiple accounts or relationships that appear to be connected for the purpose of avoiding controls; and
- any other activity identified through internal monitoring rules, alerts or reliable external information.

Higher-risk customers shall be subject to enhanced monitoring and, where appropriate, enhanced due diligence.

The Company shall maintain transaction records in a form that permits reconstruction of individual transactions and supports regulatory review and investigation.

14. Preservation of Records

SelfFin shall maintain and preserve customer identification records, transaction records and other documents required under PMLA, the PML Rules, RBI directions and other applicable law. Records shall be retained for the prescribed statutory period and in a manner that permits prompt retrieval when requested by competent authorities.

Records relating to transactions shall contain sufficient information to identify the nature, amount, date, currency and parties to the transaction, as applicable. Customer identification and address records shall also be retained for the period prescribed under applicable law.

The Company shall maintain safeguards to prevent unauthorised alteration, destruction, loss or access to records and shall ensure that relevant records remain available to authorised regulators, law-enforcement agencies and other competent authorities when legally required.

15. Reporting to Financial Intelligence Unit-India (FIU-INDIA) – CTR, STR and CCR

SelfFin shall submit reports to FIU-IND in the formats and within the timelines prescribed under applicable law and FIU-IND reporting requirements.

Cash Transaction Report (CTR)

Cash transactions meeting the prescribed statutory thresholds, including transactions that are integrally connected, shall be identified and reported in accordance with the PML Rules and FIU-IND requirements. Internal systems shall aggregate connected transactions where required for reporting.

Suspicious Transaction Report (STR)

Where SelfFin determines that a transaction or series of connected transactions is suspicious in nature, whether completed, attempted or otherwise covered by applicable reporting requirements, an STR shall be filed with FIU-IND within the prescribed period. The Principal Officer shall record the basis for treating the activity as suspicious and ensure that reporting is not unduly delayed.

Counterfeit Currency Report (CCR)

Where counterfeit currency is detected and the reporting requirement applies, SelfFin shall make the prescribed report to FIU-IND or other competent authority within the applicable timeline.

The Company shall maintain strict confidentiality regarding reports and information submitted to FIU-IND and shall ensure that no person improperly discloses the fact or substance of an STR or related investigation to the customer or any unauthorised person (tipping-off).

16. Other Essential Aspects Related to CTR and STR Reporting

- Only transactions falling within the scope of the applicable reporting requirements shall be included in CTRs, and transactions between internal Company accounts shall be treated in accordance with applicable rules.
- Cash transactions that appear to be integrally connected shall be aggregated for the purpose of determining the applicable reporting threshold.
- Transactions that are attempted, aborted or otherwise not completed may still require STR reporting where the applicable law or FIU-IND guidance requires reporting.
- Suspicious activity shall be assessed using the regulatory definition and SelfFin's internal AML monitoring framework.
- Where an STR is filed, the Company shall continue to apply appropriate risk-based controls and shall not disclose the reporting to the customer.
- SelfFin shall ensure that required information is reported accurately and within the prescribed timelines.

17. Monitoring & Reporting of Transactions

The Company shall maintain a continuous monitoring framework to identify behaviour that may indicate fraud, money laundering, terrorist financing or other unlawful activity. Illustrative indicators may include:

- reluctance or inability of the customer to satisfactorily confirm identity or provide requested information;
- transactions inconsistent with the stated purpose or expected use of the facility;
- customer activity that does not align with the customer's known financial profile;
- repayment patterns that appear unusual, including repeated cash repayment or unexplained third-party payments;
- frequent transactions involving unusual counterparties or rapid movement of funds;
- transactions showing unusually high value, frequency or complexity without an apparent legitimate rationale; and
- any other activity generating a monitoring alert or otherwise raising a reasonable suspicion.

SelfFin shall maintain appropriate transaction-monitoring limits and scenarios based on product, customer and risk characteristics. Alerts and exceptions shall be reviewed and escalated in accordance with internal procedures.

Information relating to reportable transactions and significant monitoring outcomes shall be submitted to the Principal Officer and/or relevant compliance function within the prescribed internal timelines.

18. Risk Management

SelfFin shall maintain an effective KYC/AML risk-management framework supported by coordination, communication and understanding across the Company. The Board and senior management shall ensure that adequate systems, controls, staffing and training are available for effective implementation.

- The compliance function shall periodically review KYC/AML controls and identify gaps requiring corrective action.
- Internal or independent audit functions shall test KYC/AML compliance at appropriate intervals and report material observations to the designated governance forum.
- Customer identification information, transaction records and relevant CDD information shall be available to the Principal Officer and authorised personnel on a timely basis.

- Employees shall receive periodic training on KYC, AML, CFT, sanctions, transaction monitoring, escalation and confidentiality requirements.
- Any material weakness or significant compliance issue shall be escalated to senior management and/or the Board as appropriate.

Risk categories

- Customer risk – the possibility that a customer’s characteristics or behaviour may expose Selfin to AML/CFT risk.
- Operational risk – the risk arising from inadequate or failed processes, systems, people or external events.
- Legal risk – the possibility of loss arising from legal proceedings, regulatory action, adverse judgments or non-compliance.
- Concentration/reputational risk – the risk that a concentration of exposure or adverse association could cause financial, legal or reputational harm.

19. Updation / Periodic Updation of KYC

Selfin shall periodically update customer KYC information in accordance with applicable RBI requirements and the customer’s risk category. Higher-risk customers shall be subject to more frequent review than lower-risk customers where required by applicable rules or the Company’s risk framework.

KYC records shall also be updated when material changes occur in customer identity, address, ownership/control, business activity, risk profile or other relevant information, or when the Company has reason to doubt the accuracy or adequacy of existing information.

20. Compliance of KYC Policy

Selfin shall ensure that the KYC/AML policy is implemented through appropriate governance and control arrangements, including:

- clear assignment of responsibility for KYC/AML compliance;
- independent or suitably segregated compliance testing, as appropriate;
- periodic review of compliance with KYC/AML requirements;
- appropriate reporting of material compliance exceptions to senior management and the Board;
- independent assessment or audit of KYC/AML controls at appropriate intervals; and
- submission of material compliance findings and corrective actions to the relevant governance forum.

The Company’s KYC/AML governance shall be aligned with the applicable RBI Master Direction on KYC and the requirements of the PMLA and PML Rules, as amended from time to time.

21. Policy Implementation Guidelines**Customer Education**

Selfin shall provide customers with clear information regarding the purpose of KYC, the documents required, the importance of providing accurate information and the circumstances in which updated information may be requested. Customer information shall be used only for legitimate and permitted purposes.

Introduction of New Technologies

Before adopting new technology, products, channels or processes, SelfFin shall assess the associated AML/CFT and fraud risks and introduce appropriate controls. Technology shall not be deployed in a manner that weakens customer identification, transaction monitoring or reporting controls.

Applicability to Branches and Subsidiaries Outside India

Where SelfFin has branches, subsidiaries or other operations outside India, applicable local KYC/AML/CFT requirements shall also be considered. Where local requirements are less stringent than applicable Indian standards, SelfFin shall apply the higher standard to the extent legally permissible.

KYC Policy for Existing Customers

Existing customers shall continue to be monitored and subjected to KYC review and periodic updation based on risk. Where material deficiencies are identified, SelfFin shall seek the required information and may take appropriate risk-based action if the customer does not cooperate.

Where a customer fails to provide information necessary to comply with KYC requirements, SelfFin may restrict services, decline transactions, or take other lawful measures after considering the circumstances, customer risk and applicable regulatory requirements.

22. Appointment of Principal Officer and Role of Principal Officer

SelfFin shall designate a senior management officer as the Principal Officer for AML/CFT and PMLA compliance, as required by applicable law.

The Principal Officer shall have appropriate authority, independence and access to information necessary to discharge the role and shall be responsible for:

- overseeing implementation of the KYC/AML/CFT framework;
- ensuring timely submission of required reports to FIU-IND;
- reviewing and escalating suspicious activity;
- maintaining appropriate liaison with FIU-IND, regulators, law-enforcement agencies and other competent authorities;
- ensuring appropriate confidentiality in relation to STRs and related information;
- coordinating with business, operations, compliance, risk and audit functions; and
- reporting significant KYC/AML matters to senior management and the Board, as appropriate.

23. Money Laundering and Terrorist Financing Risk Assessment and Monitoring of Risk – Adopting Risk Based Approach

SelfFin shall periodically conduct and document an enterprise-wide assessment of money-laundering and terrorist-financing risks associated with its customers, products, services, delivery channels and geographic exposure. The assessment shall be proportionate to the nature, size and complexity of the Company's business.

The risk assessment shall identify and evaluate relevant threats and vulnerabilities and shall consider customer, product, geographic, transactional, delivery-channel and other relevant risk factors. The frequency of review shall be determined based on the risk profile and shall be at least as frequent as required by applicable regulation.

The outcome of the risk assessment shall be documented, approved at the appropriate governance level and used to strengthen customer due diligence, transaction monitoring, staffing, training, systems and other controls.

SelfFin shall use a risk-based approach to determine the intensity of customer due diligence and monitoring. Higher-risk customers shall receive enhanced scrutiny, while lower-risk customers may be subject to simplified measures where permitted by law.

The Company shall review the effectiveness of the risk-based framework and make changes where material changes in business, regulation, customer profile or threat environment are identified.

24. Combating Financing of Terrorism

SelfFin shall maintain controls to prevent its products, services and channels from being used to finance terrorism or to facilitate transactions involving persons or entities subject to sanctions or other prohibitions.

- Screen customers, beneficial owners and relevant counterparties against applicable sanctions and prohibited lists.
- Pay particular attention to transactions that present unusual patterns or links to jurisdictions or persons associated with terrorist financing risk.
- Escalate potential matches or material alerts to the appropriate compliance function and Principal Officer.
- Submit required reports to FIU-IND and/or other competent authorities in accordance with law.
- Maintain confidentiality and avoid tipping-off when dealing with suspicious activity or regulatory reporting.

Where a customer or transaction is found to be connected with a designated person or entity, SelfFin shall take action in accordance with the applicable sanctions regime, PMLA, UAPA and other relevant laws and regulatory directions.

25. Countries which do not or insufficiently apply the FATF recommendations

SelfFin shall consider relevant Financial Action Task Force (FATF) statements, public notices and applicable regulatory guidance relating to jurisdictions identified as presenting strategic deficiencies in AML/CFT controls.

- Transactions and relationships involving higher-risk jurisdictions shall receive appropriate enhanced scrutiny.
- Additional customer information, source-of-funds information or other due diligence may be required where warranted by the risk.
- SelfFin shall not automatically reject every customer or transaction solely because of a jurisdictional connection unless required by law or internal policy; instead, the relationship shall be assessed in accordance with the applicable risk framework.
- Transactions involving sanctioned jurisdictions, persons or entities shall be handled in accordance with applicable sanctions and legal requirements.

26. Inter-Governmental Agreement (IGA) with United States of America (US) under Foreign Account Tax Compliance Act (FATCA) – Registration

Where Selfin is required to comply with the Foreign Account Tax Compliance Act (FATCA), Common Reporting Standard (CRS) or other applicable tax-information reporting framework, the Company shall obtain and maintain the information necessary to determine customer tax residency and reporting status.

Selfin shall comply with applicable registration, due-diligence, reporting, record-keeping and certification requirements and shall furnish information to the competent authority in the prescribed manner and within the applicable timelines.

Customer information obtained for FATCA/CRS purposes shall be handled in accordance with applicable law and the Company's privacy and data-security requirements.

27. Constitution of Special Investigating Team – Sharing of Information

Selfin shall provide appropriate cooperation and assistance to competent authorities and special investigating teams where a lawful request or investigation relates to money laundering, terrorist financing, fraud or other financial crime.

Such cooperation may include sharing customer, transaction, KYC, account or other relevant records where disclosure is required or permitted by law. Information shall be shared securely, accurately and only with authorised persons or authorities.

The Company may establish internal investigation or escalation arrangements where required to examine material suspicious activity, regulatory concerns or potential financial crime. Employees shall cooperate with such investigations and maintain required confidentiality.

Annexure A – Indicative List for Risk Categorization

The following categories are illustrative indicators for enhanced-risk classification. They are not exhaustive and shall be considered together with the customer's overall profile, transaction behaviour and other relevant information.

High Risk – Illustrative Indicators

- Individuals or entities appearing on applicable United Nations Security Council sanctions or other legally binding prohibited lists.
- Individuals or entities identified by competent authorities, regulators, law-enforcement agencies or reliable sources as being associated with serious criminal activity, terrorism or financial crime.
- Customers with unusually complex, opaque or layered ownership structures without a clear legitimate business rationale.
- Politically Exposed Persons (PEPs), their family members or close associates, where enhanced measures are required.
- Non-face-to-face or otherwise higher-risk relationships where adequate controls cannot fully mitigate the risk.
- Customers with significant or unexplained cash-intensive activity.
- Customers or counterparties with material exposure to higher-risk jurisdictions.

- Trusts, foundations, charities or similar structures where the source and application of funds are unclear or otherwise present elevated risk.
- Customers operating in sectors or activities identified through the Company's risk assessment as presenting elevated AML/CFT risk.
- Customers whose transaction behaviour is inconsistent with their known profile or economic purpose.
- Customers with adverse information suggesting fraud, money laundering, terrorist financing or other serious financial crime concerns.

Medium Risk – Illustrative Categories

- Stock brokers and securities-related businesses.
- Import/export or cross-border trading activities.
- Gas stations and other cash-intensive retail businesses.
- Car/boat or other high-value dealerships.
- Electronics wholesalers or retailers.
- Travel agencies.
- Telemarketing businesses.
- Telecommunication service providers, internet cafés or similar businesses with relevant transaction exposure.

Low Risk – General Category

Customers other than those presenting medium or high-risk characteristics may generally be treated as lower risk where their identity, source of funds and expected activity can be satisfactorily established and their transactions remain consistent with the customer profile. The Company shall nevertheless apply all mandatory KYC requirements and ongoing monitoring applicable to such customers.

Policy Governance

This Policy shall be reviewed periodically and whenever there are material changes in applicable law, RBI directions, PMLA/PML Rules, FATF standards, FIU-IND reporting requirements, the Company's products or risk profile. Any amendments shall be approved through the Company's prescribed governance process.