POLICIES & GUIDELINES

Category III AIF

SKYRIDGE FUND MANAGERS LLP

SKYRIDGE FUND MANAGERS LLP

Privacy Policy

Category III Alternative Investment Fund (AIF)
Regulatory Framework: SEBI AIF Regulations, IT Act, PMLA, DPDP (if applicable)

1. Objective

This Privacy Policy is intended to protect the personal and financial information of investors, clients, employees, and other stakeholders of Skyridge Investment Trust, a SEBI-registered Category III AIF. It outlines principles for data collection, use, storage, and sharing in line with Indian law and SEBI regulations.

2. Legal Framework

This policy is based on:
- SEBI (AIF) Regulations, 2012
- Prevention of Money Laundering Act, 2002
- Information Technology Act, 2000
- Draft Digital Personal Data Protection Act, 2023
- Applicable global privacy principles such as GDPR (where relevant)

3. Scope

This policy applies to:
- Investors and prospective investors
- Directors, employees, officers, and consultants
- Intermediaries and service providers handling personal or financial data

4. Types of Personal Data Collected

- Name, DOB, address, contact details
- PAN, Aadhaar, Passport, or government-issued IDs
- Bank and investment details
- KYC, tax info, and IP/device data

5. Purpose of Data Collection

We collect personal data to:
- Comply with KYC and SEBI onboarding requirements
- Administer investor relationships

- Meet audit, legal, and compliance obligations
- Improve communication and support

6. Lawful Basis for Processing

We process data when:
- Consent is provided
- Required for legal compliance
- Necessary for contract execution
- Legitimate business interests apply

7. Data Disclosure and Sharing

We may share data with:
- SEBI, FIU-IND, or regulators
- Legal, audit, or tax advisors
- Authorized third-party vendors (e.g., KYC, IT services)
- Only on a strict need-to-know basis

8. Data Retention

- Investor data: minimum 5 years post relationship
- Employee data: up to 8 years after exit
- Retention aligned with SEBI/PMLA compliance

9. Data Protection and Security Measures

- Role-based access and encryption
- Firewalls, antivirus, and security audits
- Employee training and physical safeguards

10. Individual Rights

Individuals have the right to:
- Access and correct data
- Withdraw consent (subject to law)
- Request deletion/restriction
- File complaints with the DPO or authorities

11. Data Breach Reporting

In case of breach:
- Prompt internal reporting

- Notify SEBI or CERT-In as required
- Inform affected persons where relevant

12. Third-Party Relationships

- Third parties must sign DPAs
- Due diligence on vendors' security practices
- Regular audits of external data handlers

13. Policy Review and Amendments

Policy reviewed annually or upon legal changes. Approved changes are communicated to stakeholders.

14. Contact Details

Compliance Officer
Vishakha Karnani
vishakha@skyridgefund.com

15. Approval

Approved by:
Board of Directors – Skyridge Fund Managers LLP
Abhishek Maheshwari – Principal Officer
Vishakha Karnani – Compliance Officer
Date: 15th March 2025

SKYRIDGE FUND MANAGERS LLP

Employee Screening Policy

Category III Alternative Investment Fund (AIF)
Regulatory Framework: SEBI AML/CFT Guidelines & PMLA, 2002

1. Objective

This policy establishes the employee screening standards of Skyridge Investment Trust to ensure that only individuals with the necessary integrity, competence, and background are employed or contracted, particularly in roles that impact regulatory compliance, fund management, investor services, and risk management. The screening process helps safeguard against financial crime risks, including money laundering, terrorist financing, and proliferation financing.

2. Scope

This policy applies to:

- All full-time and part-time employees
- Temporary/contractual staff
- Designated Partners and key managerial personnel
- Employees of outsourced service providers handling sensitive information or transactions

3. Screening Requirements

3.1 Pre-Employment Screening

Before confirming employment, the following checks must be conducted:

Check Type	Applicable to	Description
Identity Verification	All candidates	Government-issued ID (e.g., Aadhaar, PAN)
Educational Background	All mid- to senior-level roles	Verify highest qualification from issuing institution
Employment History	All roles	Minimum last 3 years' employment checks
Criminal Record Check	All roles	Declaration and verification (including police clearance for sensitive roles)

Reference Check	Mid- to senior-level roles	Minimum two professional references
Credit and Financial Check	Compliance, risk, finance personnel	Ensure no significant default or adverse financial history

3.2 Ongoing Screening

- Periodic Rescreening: Every 2–3 years for critical roles (e.g., fund management, compliance, operations)
- Continuous Watchlist Monitoring: Names of all employees in sensitive roles to be periodically screened against updated UN and national sanctions lists

4. Roles and Responsibilities

Role	Responsibility
HR Department	Execute background checks and maintain records
Compliance Officer	Oversee sanctions list and regulatory-related screenings
Principal Officer	Ensure alignment with AML/CFT/PF framework
Hiring Managers	Ensure role-based screening is completed before onboarding

5. Record Keeping

- All screening records (documents, reports, verifications) will be retained for at least 5 years after cessation of employment
- Access to records will be limited to authorized personnel only and subject to confidentiality

6. Confidentiality and Data Protection

- All screening information shall be collected and processed in compliance with applicable data protection laws in India
- Consent from the employee/applicant will be taken before initiating checks

7. Non-Compliance

Failure to complete the required screening prior to onboarding or to address discrepancies may result in:

- Delayed or revoked offers of employment
- Internal investigation or disciplinary action
- Reporting to regulatory authorities in extreme cases

8. Policy Review

This policy will be reviewed annually, or as required due to regulatory changes or internal risk assessment outcomes. Updates shall be approved by senior management or the Board.

Approved by:
Board of Partners – Skyridge Fund Managers LLP
Vishakha Karnani – Compliance Officer
Abhishek Maheshwari – Principal Officer
Date: 15th March 2025
Place: Mumbai

SKYRIDGE FUND MANAGERS LLP

Customer Due Diligence (CDD) Policy

Category III Alternative Investment Fund (AIF)
Regulatory Framework: SEBI AML/CFT Guidelines & PMLA, 2002

1. Objective

The primary objective of this Customer Due Diligence (CDD) Policy is to establish a framework for verifying the identity of investors and ensuring that no funds are raised from or linked to individuals or entities involved in illegal activities, including money laundering or terrorism financing. The policy aims to meet the regulatory requirements under the PMLA, 2002, and SEBI guidelines while ensuring the protection of investors' interests.

2. Regulatory Framework

This policy is framed based on the following:

- SEBI (Alternative Investment Funds) Regulations, 2012
- Prevention of Money Laundering Act (PMLA), 2002
- FATF Recommendations
- SEBI Master Circular on AML/CFT (October 12, 2023)
- Guidelines issued by the Financial Intelligence Unit (FIU-IND)

3. Scope

This policy applies to:

- All investors in the AIF (individuals, corporate entities, partnerships, trusts, etc.)
- All employees, officers, and KMP involved in the onboarding, monitoring, and reporting of investors
- Third-party intermediaries involved in KYC and CDD processes

4. Customer Due Diligence (CDD) Process

4.1 Know Your Customer (KYC) Requirements

Before onboarding any investor, the following steps must be undertaken:

4.1.1 Investor Identification

- Individual Investors: Full name, date of birth, nationality, and residential address. Valid government-issued ID (e.g., Aadhaar, PAN, Passport, Voter ID) and a proof of address (e.g., utility bill, bank statement).

- Corporate Investors: Full legal name, registration number, registered address, business type, nature of activity, and ownership structure. Relevant documents include Certificate of Incorporation, Memorandum & Articles of Association, PAN, and board resolution authorizing the investment.
- Trusts, Partnerships, and Others: Trust deed, partnership agreement, and other related documents.

4.1.2 Verification of Identity

- Use of independent sources such as government databases, financial institutions, or third-party KYC platforms for verification.
- Periodic re-verification of identity at least once every 3–5 years for high-risk investors.

4.2 Risk-Based Approach

- Low-Risk Investors: Standard KYC checks and verification. Monitoring based on transactional activity.
- Medium-Risk Investors: Enhanced due diligence (EDD) including additional checks on source of funds and wealth.
- High-Risk Investors: Thorough background checks, including verification against sanction lists (UNSC, FATF, SEBI), politically exposed persons (PEPs) screening, and source of funds and wealth checks. Regular monitoring and reporting of transactions.

4.3 Enhanced Due Diligence (EDD) for High-Risk Clients

For clients categorized as high-risk, the following procedures must be followed:

- Obtain detailed information regarding the investor's source of wealth and source of funds.
- Perform detailed checks for negative news, legal actions, and involvement in criminal activities.
- Obtain independent verification from trusted third-party sources where applicable.
- Ensure ongoing monitoring of the relationship with periodic reviews every 6–12 months.

4.4 Politically Exposed Persons (PEPs)

- Identification of PEPs: All investors must be screened against international PEP databases.
- Additional Measures for PEPs: When dealing with PEPs, enhanced due diligence is mandatory, including identifying the source of wealth, the source of funds, and close family members and associates.

5. Ongoing Monitoring and Reporting

5.1 Transaction Monitoring

- Continuous monitoring of investor transactions to detect unusual or suspicious activity.

- Automated tools may be used to flag unusual transactions that deviate from expected patterns (e.g., large, complex, or unusual transactions).
- Suspicious Transaction Reporting (STR): If any suspicious transaction is identified, it must be reported immediately to the Principal Officer, who will forward the report to the Financial Intelligence Unit (FIU-IND).

5.2 Record Keeping

- Maintain investor-related documentation (KYC, due diligence reports, communications, etc.) for at least 5 years after the business relationship is terminated.
- Ensure records are easily retrievable and made available for regulatory review.

6. Third-Party Intermediaries

- Outsourcing of KYC Services: If third-party service providers (e.g., KYC verification agencies) are used for the investor identification process, the AIF must ensure that these providers comply with PMLA, SEBI regulations, and other applicable laws.
- Due Diligence of Intermediaries: Ensure that any third-party intermediary used for investor screening, KYC, or CDD complies with the standards set in this policy.

7. Compliance Officer and Principal Officer

- Compliance Officer: Responsible for ensuring the implementation of this CDD policy, conducting regular audits of the KYC process, and reporting non-compliance to the Board.
- Principal Officer: The designated Principal Officer is responsible for submitting Suspicious
- Transaction Reports (STRs) to the FIU-IND and ensuring that the organization follows AML/CFT regulations.

8. Training and Awareness

- All employees involved in the onboarding, monitoring, and reporting of investors will undergo mandatory training on CDD, KYC, and AML/CFT policies.
- Training must be conducted at least annually and updated as per changes in regulations or risk assessments.

9. Non-Compliance and Penalties

- Failure to Comply: If an investor refuses to provide the necessary KYC information or documentation, the AIF may refuse to accept the investment or terminate the existing relationship.
- Disciplinary Action: Employees who fail to follow the CDD procedures may face disciplinary action, including suspension or termination.

10. Review and Amendments

– This policy will be reviewed at least annually, or sooner if there are changes in SEBI regulations, PMLA guidelines, or internal risk assessments.
– Any amendments to this policy must be approved by the Board of Directors.

Approved by:
Board of Partners – Skyridge Fund Managers LLP
Vishakha Karnani – Compliance Officer
Abhishek Maheshwari – Principal Officer
Date: 15th March 2025
Place: Mumbai

SKYRIDGE FUND MANAGERS LLP

Training of Employees Policy – AML/CFT/PF

Category III Alternative Investment Fund (AIF)
Regulatory Framework: SEBI Master Circular on AML/CFT & PMLA, 2002

1. Objective

The objective of this policy is to ensure that all employees of Skyridge Investment Trust, particularly those in compliance, operations, risk management, and investor relations, are trained and made aware of their obligations under the applicable AML/CFT/PF regulatory framework. The policy also seeks to foster a culture of compliance and vigilance against financial crimes, in line with SEBI guidelines and the PMLA.

2. Scope

This policy applies to:

- All full-time and part-time employees
- Key managerial personnel
- Fund managers, compliance staff, and operations personnel
- Any third-party service providers involved in investor onboarding, KYC, or transaction processing (e.g., RTA, custodians)

3. Training Components

Employees shall be trained on the following core topics:

A. AML (Anti-Money Laundering)

- Overview of the Prevention of Money Laundering Act, 2002 (PMLA)
- SEBI AML/CFT requirements
- Customer Due Diligence (CDD), KYC, and identification of Ultimate Beneficial Owners (UBOs)
- Monitoring and recognizing suspicious transactions
- Reporting obligations and internal escalation

B. CFT (Combating the Financing of Terrorism)

- Nature and methods of terrorist financing
- Red flags and high-risk jurisdictions (FATF watch lists)
- Obligations related to reporting and due diligence for terrorist financing risks

C. PF (Proliferation Financing)

- Definition and risks associated with proliferation of weapons of mass destruction
- United Nations Security Council (UNSC) sanctions and lists
- Screening requirements against sanctioned individuals and entities
- SEBI's requirement for PF-related training and record keeping

4. Training Frequency and Format

Category of Employee	Frequency
All Staff	Annual
New Employees	Within 30 days of joining
Compliance & Operations	Semi-Annually
Senior Management	Annual

5. Roles and Responsibilities

Role	Responsibilities
Compliance Officer	Develops, coordinates, and monitors AML/CFT/PF training programs
Principal Officer (PO)	Ensures content is updated per FIU-IND and SEBI guidelines
Employees	Responsible for attending training sessions and applying knowledge in daily operations

6. Training Records and Documentation

- Training attendance, modules, materials, and assessments will be maintained for at least 5 years.
- Records shall be made available to SEBI or FIU-IND upon request.
- Completion confirmations and refresher reminders shall be generated through the internal HR or compliance system.

7. Evaluation and Effectiveness Review

- Participants may be required to complete assessments or quizzes post-training.
- Feedback will be collected to improve future sessions.
- The effectiveness of the training program will be reviewed annually by the Compliance Committee.

8. Non-Compliance

- Failure to attend or complete mandatory training without valid reason may be recorded in the employee file.
- Repeated non-compliance may lead to disciplinary action in line with policy.

9. Policy Review and Updates

This policy will be reviewed annually or earlier if there are significant changes in the regulatory framework or operational practices. Updates will be approved by the Board or the designated authority.

Approved By:
Board of Partners – Skyridge Fund Managers LLP
Vishakha Karnani – Compliance Officer

SKYRIDGE FUND MANAGERS LLP

Abhishek Maheshwari – Principal Officer
Date: 15th March 2025
Place: Mumbai

SKYRIDGE FUND MANAGERS LLP

Policy on Prevention, Detection, and Reporting of Suspicious Transactions

Category III Alternative Investment Fund (AIF)
Regulatory Framework: SEBI Master Circular on AML/CFT and PMLA, 2002

1. Objective

To establish a robust and SEBI-compliant Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) framework to prevent, detect, and report suspicious transactions in accordance with the Prevention of Money Laundering Act, 2002 (PMLA) and rules made thereunder, and the SEBI Master Circular dated October 06, 2023, and subsequent updates.

2. Applicability

This policy is applicable to:

- The AIF and its Investment Manager
- Trustees and Designated Partners (if applicable)
- Fund employees and intermediaries
- Portfolio Managers and Custodians engaged by the AIF

3. Key Roles and Responsibilities

Role	Responsibility
Designated Partners/KMPs	Overall compliance with the obligations under the PMLA.
Principal Officer (PO)	Acts as the nodal person for AML matters, including reporting of Suspicious Transaction Reports (STRs) to FIU-IND.
Compliance Officer	Implements, monitors, and ensures ongoing adherence to AML/CFT procedures. Coordinates employee training and internal controls.

4. Client Due Diligence (CDD)

As per SEBI Master Circular and PMLA, the AIF shall:

- Carry out KYC through KRA and CKYC for all investors prior to onboarding.
- Collect PAN, proof of identity, address, financial details, and beneficial ownership information.
- Conduct Enhanced Due Diligence (EDD) for high-risk categories such as PEPs, non-face-to-face clients, or those from FATF non-cooperative jurisdictions.
- Maintain updated records and perform periodic reviews.

5. Identification of Suspicious Transactions

Suspicious indicators include but are not limited to:

- Large or inconsistent investments not in line with declared income or profile.
- Frequent fund transfers between jurisdictions, especially from FATF-flagged countries.
- Investments without clear economic purpose or that involve layering of funds.
- Attempts to obscure the identity of the ultimate beneficial owner (UBO).

The AIF shall develop an internal list of Red Flag Indicators as recommended by SEBI and FIU-IND.

6. Monitoring and Detection Mechanism

- Risk-Based Monitoring shall be implemented across investor transactions.
- High-risk clients shall be subject to enhanced monitoring.
- Transactions flagged through internal alerts or employee reporting will be reviewed by the Compliance Team.
- Monitoring shall be both automated (where feasible) and manual, depending on the volume and risk profile.

7. Reporting of Suspicious Transactions

- Employees must escalate any suspicious transaction to the Principal Officer (PO) immediately.
- The PO, after internal assessment, shall submit a Suspicious Transaction Report (STR) to FIU-IND in the prescribed format and within 7 working days of reaching a conclusion.
- Reporting is confidential – clients are not to be informed.
- Records of all STRs must be retained securely for a minimum of 5 years.

8. Training and Awareness

- Mandatory AML/CFT training will be conducted for employees annually.
- Training shall cover:
  - KYC/UBO identification
  - Detection of suspicious activity
  - Reporting procedures
  - Legal implications under PMLA/SEBI

- Records of training must be maintained.

9. Record Maintenance

As mandated by Rule 3 of PML Rules, 2005, the AIF must:

- Retain investor KYC and transactional records for at least 5 years from the end of the business relationship.
- Maintain a register of STRs and internal investigations.
- Make such records readily available for inspection by SEBI or FIU-IND.

10. Internal Audit and Review

- The internal audit team, if any, shall periodically verify adherence to the AML framework.
- Any deficiencies or non-compliance shall be reported to the Board and SEBI where necessary.
- The policy will be reviewed annually or upon significant regulatory changes.

Approved By:
Board of Partners – Skyridge Fund Managers LLP
Vishakha Karnani – Compliance Officer
Abhishek Maheshwari – Principal Officer
Date: 15th March 2025
Place: Mumbai

SKYRIDGE FUND MANAGERS LLP

Red Flag Indicators Recommended by SEBI and FIU-IND

Category III Alternative Investment Fund (AIF)

The **red flag indicators** for suspicious activity in relation to **Anti-Money Laundering (AML)** and **Combating the Financing of Terrorism (CFT)** are crucial in detecting potential illegal activities like money laundering and terrorist financing. Both the **Securities and Exchange Board of India (SEBI)** and the **Financial Intelligence Unit - India (FIU-IND)** provide guidelines to help financial institutions and intermediaries (such as Category III AIFs) in identifying such activities. Below are the key **red flag indicators** as recommended by SEBI and FIU-IND:

1. Unusual/Complex Transactions

- Transactions that do not appear to have a clear or legitimate business or economic purpose.
- Transactions that appear to be unusually large, complex, or structured to avoid detection or reporting requirements.
- Transactions inconsistent with the investor's usual behavior or profile.

2. Unexplained or Unjustified Use of Third Parties

- The involvement of third parties in transactions where the investor has no clear relationship with them, or the third parties' identities are difficult to verify.
- Investors acting on behalf of another person, without adequate documentation or clarity.

3. Reluctance to Provide Information

- The investor's unwillingness to provide required documentation (e.g., KYC, source of funds, or source of wealth).
- Investors or clients providing false or misleading information during the onboarding process.
- The investor requests for secrecy or confidentiality beyond normal business confidentiality practices.

4. Source of Funds or Wealth Not Justified

- Investors unable or unwilling to explain the source of their funds, especially when dealing with large transactions.
- Investment from an individual or entity whose financial standing is inconsistent with the volume or nature of the transactions.

- The use of offshore accounts or entities located in jurisdictions known for money laundering, tax evasion, or terrorism financing.

5. Transactions with High-Risk Countries or Jurisdictions

- Transactions involving countries or jurisdictions that are known for inadequate AML/CFT regulations, or those that are subject to international sanctions.
- Transfers or investments in/from high-risk countries or countries under international scrutiny (e.g., those included in the FATF's high-risk or non-cooperative jurisdictions list).

6. Frequent and Unnecessary Changes in Investment or Account Details

- Frequent changes in the nature of the investor's account (e.g., frequent changes of beneficiaries, account instructions, or sources of funding).
- Sudden or large transfers of funds to or from high-risk jurisdictions or multiple countries.
- Clients switching between products or strategies without clear rationale.

7. Multiple Small or Round-Sum Deposits

- Large sums of money being deposited in small amounts to avoid detection or reporting requirements, a practice known as **structuring** or **smurfing**.
- Clients depositing or transferring money in round sums (e.g., multiple transactions of the same amount), which may indicate an attempt to mask the total value of the funds.

8. No Clear Economic or Business Purpose

- Transactions where the client cannot provide a clear and verifiable reason for the investment or transaction.
- Investments in products or assets that do not align with the client's declared objectives or investment strategy.

9. Suspicious Withdrawals

- Investors withdrawing funds shortly after they have been deposited, especially without any substantial reason.
- Early redemption of investments or liquidations in a manner that is inconsistent with the fund's expected maturity or investment horizon.

10. Irregularities in Documentation

- Gaps or discrepancies in documentation provided by the investor (e.g., mismatched signatures, missing corporate documents, unregistered addresses).
- Inconsistent or incomplete KYC documentation, particularly for corporate or high-net-worth investors.

11. Unusual Pattern of Transactions Across Different Accounts

- Funds transferred between multiple accounts without a clear or justifiable reason (e.g., from multiple clients to a single account or vice versa).
- A client using multiple accounts without clear business reasoning behind such patterns.

12. Involvement of Politically Exposed Persons (PEPs)

- A client or associated parties being categorized as Politically Exposed Persons (PEPs) or their close family members.
- If the client is identified as a PEP, enhanced due diligence must be applied, and any suspicious activity related to their transactions must be reported.

13. Over- or Under-Invoicing of Transactions

- The use of over-invoicing or under-invoicing for goods or services as a method of money laundering.
- Payments for transactions involving a business relationship that cannot be substantiated or that lack reasonable business justification.

14. Activities Inconsistent with Known Business Activities

- The volume or type of transactions being inconsistent with the known business or economic activities of the client.
- If an investor engages in an activity that is outside the scope of their declared business, the transaction could be suspicious.

15. Involvement of Shell Companies or Complex Ownership Structures

- Transactions involving shell companies or entities with opaque or complex ownership structures designed to obscure the identity of the true beneficial owners.
- Lack of transparency in the ownership structure of entities involved in the transaction.

SEBI Guidelines on Reporting Suspicious Transactions

SEBI emphasizes the following in its regulatory framework for AIFs:

- **Reporting Suspicious Transactions**: SEBI mandates AIFs to report suspicious transactions promptly to the **Principal Officer** who will forward them to the **Financial Intelligence Unit – India (FIU-IND)**.
- **Compliance with AML Regulations**: AIFs must establish robust systems to monitor and report suspicious activities, in accordance with PMLA requirements.
- **Employee Training**: Staff must be trained to recognize red flags and respond appropriately to suspicious activities.

FIU-IND Guidelines

The **Financial Intelligence Unit - India (FIU-IND)** also recommends vigilance regarding the following:

- The **filing of Suspicious Transaction Reports (STR)** for transactions that show suspicious patterns or do not match the risk profile of the client.
- Regular screening of investors against the **List of Individuals and Entities** identified by FATF and other relevant global watchlists.

By keeping a close eye on these indicators, Category III AIFs can help prevent, detect, and report suspicious activities in compliance with the regulatory framework, thereby mitigating the risks of money laundering and terrorism financing.