Dowell FISCAL Services Private Limited

Department: Compliance

Versions: DFSPL/ FY-2023-24/ Nov /KYC Policy/Version:2.0
Effective Date: 04/01/2024

Know Your Customers (KYC) and Prevention of Money Laundering (PML) Policy

EXECUTIVE SUMMARY

The primary objective of "***Know Your Customer***" (KYC) policy is to prevent Dowell Fiscal Services Ltd. (DFSPL) from being used, intentionally or otherwise, by unscrupulous elements for fraudulent/money laundering and terrorist financing activities as enunciated in the "***Customer Acceptance Policy*** "of DFSPL and various circulars issued by the Reserve Bank of India (RBI) on the subject matter from time to time. KYC procedures also enable to know/understand customers and their financial dealings better which, in turn, help to manage their risks prudently.

1. INTRODUCTION

The Reserve Bank of India (RBI) had issued Master Direction vide DBR.AML.BC.No.81/14.01.001/2015-16. February 25, 2016 (updated as on January 04, 2024) and amendment to master direction no DOR/AML/REC No 15/14.01.001/2021-22 dated May 10, 2021 under Prevention of Money-Laundering Act, 2002 and Prevention of Money-laundering (Maintenance of Records) Rules, 2005. Based on the above framework provided by RBI, KYC policy has been drafted incorporating the Standard Operating Procedures on KYC and AML requirements (hereinafter referred to as the "KYC Policy").

Important terms & definitions

1. **Applicability -** All Branches / Offices / authorized officer shall mandatorily comply with the procedures laid down by this policy. Non-compliance will be construed as misconduct on the part of the employee which will attract appropriate penal action.
2. **Transactions -** The policy will be applicable for all "Transactions" done by the company. "Transaction" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:
    a. opening of loan account;
    b. deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non- physical means;
    c. entering into any fiduciary relationship;
    d. any payment made or received, in whole or in part, for any contractual or other legal obligation; or
    e. establishing or creating a legal person or legal arrangement.

3. The policy will be applicable to all "Customers" including Applicant, Co-Applicant, Guarantor, Beneficial Owner (BO), Business Partners. "Customer" means a person who is engaged in a financial transaction or activity with the company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting. Customer will include the following:
    a. an individual,
    b. a Hindu undivided family,
    c. a company,
    d. a firm,
    e. an association of persons or a body of individuals, whether incorporated or not,
    f. every artificial juridical person, not falling within any one of the above persons (a to e), and
    g. any agency, office or branch owned or controlled by any of the above persons (a to f).

KYC documentation collection, its validation and OSV (Original Seen & Verified) check/certification as specified in this circular shall be fulfilled either in physical form, V-CIP (Video Customer Identification Process) or in digital mode.

4. **Digital Signature** shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).

5. **Equivalent e-document** means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

2. APPOINTMENT OF PRINCIPAL OFFICER (PO)

As required under the Prevention of Money Laundering Act, 2002 (PMLA), Mr. Jatin Singhal has been appointed as the Principal Officer of our Company. The Principal Officer shall *inter alia* be responsible for reporting for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the Prevention of Money Laundering Act, 2002, rules and regulations made thereunder, as amended from time to time. The name, designation and address of the Principal Officer shall be communicated to FIU-IND by Compliance/Secretarial Department. Pursuant to this clause, Legal and Compliance department shall separately notify the PO with his roles and responsibilities under KYC and PMLA.

3. APPOINTMENT OF DESIGNATED DIRECTOR

As required by Reserve Bank Mr. Rakesh Mehta has been appointed as Designated Director for ensuring compliance with the obligations under the PML Act. The name, designation and address of the Designated Director shall be communicated to FIU-IND by Compliance/Secretarial Departments.

4. **COMPLIANCE OF KYC POLICY**

4.1 CONSTITUTION OF SENIOR MANAGEMENT

As per RBI circular, the Senior Management has been constituted for KYC Policy. Senior Management shall comprise of Whole Time Directors, Chief Financial Officer, Chief Business Officer, Head Credit and Risk

4.2 CONCURRENT/INTERNAL AUDIT

Independent evaluation of the compliance functions pertaining to KYC and PMLA shall be done. It would include the verification for compliance of KYC/AML policies and procedures (both design and implementation) on a quarterly basis and highlighting the necessary modifications if any so as to ensure the compliance. Compliance report on KYC Policy shall be submitted to Audit Committee on quarterly basis.

4.3 OUTSOURCING:

Decision Making function of determining compliance with KYC Norm shall not be outsourced.

4.4 HIRING AND TRAINING

Human Resource Department shall put in place the screening mechanism as an integral part of their personnel recruitment/hiring process. HR, Legal & Compliance and Operations Department shall arrange an on-going

employee training program for the different categories of members of staff and ensure that they are adequately trained in KYC/AML procedures. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT policies of the RE, regulation and related issues shall be ensured.

4.5 CUSTOMER DUE DILIGENCE

Customer due diligence means identifying and verifying the customer and Beneficial Owner using "Officially Valid Documents" as a proof of identity and a proof of address.

4.6 CENTRAL KYC RECORDS REGISTERY

CKYCR means an entity to receive, store, safeguard and retrieve the KYC record in digital form of a customer. Operations Department has taken necessary steps to comply with the norms of CKYCR within specified timelines. Government of India authorize the Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR.

4.7 Reporting Requirement under Foreign Account Tax Compliance Act (FATCA).

Under FATCA and CRS, Finance Department shall adhere to the provisions of Income Tax Rules and accordingly take steps for complying with the reporting requirements:

- Registration to be done on the url https://incometaxindiaefiling.gov.in for filing the returns. Submit e-filling report by using digital signature of the designated director either uploading form 61B or NIL report, for which, the schema prepared by Central Board of Direct Taxes (CBDT) shall be referred to.
- Reference can be taken from www.fedai.org.in/revaluationrate.aspx for carrying out due diligence procedure for the purpose of identifying reportable accounts under section 114H of Income Tax Account.
- Help of IT framework for due diligence, for recording and maintaining the information.
- The Senior Management constituted under the Designated Director will ensure the compliancewith updated instructions/ rules/ guidance notes/ Press releases/ issued on the subject by Central Board of Direct Taxes (CBDT) from time to time and available on the web site http://www.incometaxindia.gov.in/Pages/default.aspx.
  Company may take note of the following:
  i. updated Guidance Note on FATCA and CRS
  ii. a press release on 'Closure of Financial Accounts' under Rule 114H (8).

5. The KYC policy includes following key elements

5.1 Customer Acceptance Policy

5.2 Customer Identification Procedures (CIP) – (1) Physical, (2) Video – CIP, (3) Digital - KYC

5.3 Risk Management

5.4 Customer Due Diligence (CDD) procedure as specified in Annexures

5.5 Monitoring of Transactions

5.6 Business Partner Due Diligence

5.7 Central KYC Records Registry (CKYCR)

5.8 Annexures

5.1 CUSTOMER ACCEPTANCE POLICY

(a) No account is opened in anonymous or fictitious / benami name.

(b) No account is opened where the company is unable to apply appropriate Customer Due Diligence measures (CDD), either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.

(c) No transaction or account-based relationship is undertaken without following the CDD procedure

(d) The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, shall be as specified in this procedure note.

(e) 'Optional'/additional information, is obtained with the explicit consent of the customer after the account is opened.

(f) The CDD procedure are applied at Unique Customer Identification Code level (UCIC).

(g) CDD Procedure is followed for all the joint account holders, while opening a joint account.

(h) De-dupe check should ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India. The De-dupe data base should be updated periodically by Compliance and IT Team.

5.1.A KYC PROCESS

CUSTOMER IDENTIFICATION

Every employee of DFSPL Group or DFSPL Group authorized representative as specified in respective product policies such as Dealer/ DSA/Other representatives shall establish a customer relationship only after the identity and address of the customer and all those who represent the customer has been verified and found satisfactory. Company can also utilize the manual/digital/electronic mechanism for validating Name and Address of the customer.

Step 1

The process of customer acceptance begins with interaction with the customer.

Step 2

The customer is required to complete the Application Form/Request for Loan in Physical / Digital form wherein details on the background and facilities opted by the customer are recorded. All applicable fields should be completed.

Step 3

The details furnished in the Application Form – Physical / Digital shall be supported by Photograph (applicable in case of individual) Proof of Identity and Proof of Address. The documents that can be accepted to support the identity and address of all parties signing the agreement i.e. applicant, co-applicant, guarantor and Beneficial Owner (BO) are listed in the attached Annexure A2– List of Important Instructions, Documents Accepted as OVD (Officially Valid Document) - Proof of Identity and Proof of Address**.** OVD are collected to identify the customers and confirm their stay at a particular address with the help of reliable, independent

source documents, data or information. Photograph should be a recent color passport size photograph and can be physical or digital.

Step 4

Supporting documents obtained as should be verified with originals and certified by the person verifying the same as 'True Copy' i.e. Original, Seen and Verified (OSV). The DFSPL Group Employee or DFSPL Group Representative who meets the customer should perform the verification. (OSV stamp with name, signature and employee / representative code). Same can be done in physical or digital mode.

Step 5

The Deduplication Check with DFSPL group system should be conducted. Necessary de-duplication check to be done before opening a new account as well as check to be done to ensure as far as possible that the identity of the applicant does not match with any person with known criminal background or with the willful defaulters as per the list published by the RBI or with banned entities such as individual terrorists or terrorist organizations or list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) etc. Deduplication Check (Internal Dedupe) should be mandatorily done.

Step 6

Wherever required, verification of customer information through various means such as Tele-verification/Contact Point Verification) may be conducted by DFSPL Group employee or DFSPL Group authorized representative.

5.2 Customer Identification Procedure (CIP)

5.2.1 Customer Identification Procedure (CIP) - Physical

1. The Company shall undertake identification of customers in the following cases as and when applicable:
   (a) Commencement of an account-based relationship with the customer.
   (b) Carrying out any international money transfer operations for a person who is not an account holder of the bank.
   (c) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
   (d) Selling third party products as agents, selling their own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand.
   (e) Carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.
   (f) When the Company has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.
   (g) The Company shall ensure that introduction is not to be sought while opening accounts.

2. For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, the Company, shall at its option, rely on customer due diligence done by a third party, subject to the following conditions:

(a) Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.

(b) Adequate steps are taken by the Company to satisfy itself that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.

(c) The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.

(d) The third party shall not be based in a country or jurisdiction assessed as high risk.

(e) The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the company.

5.2.2. Re-use of KYC is allowed only for Low and Medium Risk Customer, provided:

I. Customer consent is required to re-use of the existing KYC document

II. The old KYC document available is valid and comply with the applicable KYC policy as of the date of fresh login of the case, and

III. there is no change in address or customer identification, and

IV. The address mentioned in Application Form for proposed funding matches with the downloaded KYC document and

V. A declaration shall be provided by DFSPL Group Employee that the KYC has been downloaded from DMS. The employee downloading the document shall sign all KYC mentioning name, employee id, date and

VI. If the KYC has been pre-written by customer for restricted use, then fresh KYC would be required to be collected. vii. In case contact point verification / customer interaction reports that customer address / KYC detail does not match with the downloaded KYC then fresh KYC shall be obtained.

VII. Additionally, in case of Non-Individual customers the following documents are required afresh from customer / digital source -

- Company - Board Resolution, List of Directors, Latest Shareholding pattern, Power of Attorney (if applicable).
- Partnership Firm - Partnership deed/list of partners with profit sharing ratio, Partnership Authority Letter, Power of Attorney (if applicable).
- HUF – HUF Letter.
- AOP/BOI (including Trust, Society etc.) - list of members with beneficial interest percentage Resolution as per entity type, Power of Attorney (if applicable).

5.2.3 Video - Customer Identification Procedure (V-CIP / Video - KYC)

V-CIP is an alternate digital process laid down to complete the KYC requirement of Individual customer as compared Physical Customer Identification Process to gather information and documents required for CDD purpose (Customer Due Diligence). This is also called Video -KYC. Such process shall be treated equivalent to face-to-face physical process. The V – CIP need to have followed standard process steps, controls, and design:

Sr.	Parameters	Norms
1	Applicability	Individual • Live V-CIP is applicable for Individual

		Non-Individual • Proprietor in case of proprietorship firm along with the e-document of Business activity proof as defined in CDD norms, • For other Non-Individual Entity customer, the Live V-CIP shall be applicable for authorized signatories and BO customer, and • Updation / periodic updation of KYC of eligible customers.
2	Customer Consent	• The explicit customer consent is required before V-CIP is undertaken.
3	Execution of V-CIP	• The official of DFSPL Group shall carry out the live V-CIP process with customer.
	PAN Verification	• Clear Image of PAN card/e-PAN to be captured while customer display it during V-CIP, and • Mandatory PAN verification from the government data source through suitable vendor API.
4	Recording of Video & Photograph	• The employee shall record video and capture live photograph snapshot of the customer present for V-CIP.
5	Video recording Quality and Geo Tagging	• The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. • The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.
6	Face Liveliness	• The V-CIP application shall have components with face liveness, spoof detection as well as face matching technology with high degree of accuracy. • The company will use the advance technology including artificial intelligence for various matching (such as facial match etc) to ensure integrity of V-CIP. • Inspite above, the final responsibility of customer identification shall rest with the company.
7	Customer Identification through Aadhaar XML Verification	• Offline Aadhaar Verification shall be required during V-CIP. The Aadhaar XML and Secure code should not be more than 3 days older than date of V-CIP date. • If image of Aadhaar document is stored the Aadhaar no. should be blacked out /redacted. • The address on Aadhaar should match with the current address of the customer otherwise normal physical KYC can be executed unless a functionality is developed on the system to capture defined additional document of current address proof. Further, once system capability is developed the following other method of customer identification can be executed: • KYC records downloaded from CKYCR, in accordance, using the KYC identifier provided by the customer, or • Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digi Locker.
8	Photo Match	• The live photo captured during V-CIP should match with the photo retrieved from PAN and Aadhaar authorities through digital mode. • The matching algorithm to give matching percentage and employee should confirm the photo match. • Threshold of the photo match to be decided by Risk and RCU and modify time to time based on learnings.
9	Name Matching logic	• Name matching logic to be in inbuilt in system between the name received from PAN API and Aadhaar XML.

10	Security Questions	• In order to have a liveliness check of the customer during V-CIP the employee shall ensure the sequence and/or type of questions are varied in order to establish that the interactions are real-time and not pre-recorded.
11	V-CIP De-dupe check	• The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be rejected.
12	Concurrent Audit	• The concurrent audit shall be mandatory for completion of each V-CIP. • The audit shall be done by employee of a different department as decided by management from time to time, such as Operations, CPC, RCU etc.
13	IT Security	• The V-CIP shall be seamless, real-time, secured, end-to-end encrypted audio-visual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt. • The system should be robust enough to guard against spoofing, any other fraudulent manipulations. • The software & security audit & validation should be conducted before launch by competent authority. • Minimum baseline cyber security and resilience framework to be prepared by IT dept. and shall be updated from time to time as well as other general guidelines on IT risks.
14	Company Domain	The technology infrastructure should be housed in own premises of the DFSPL Group and the V-CIP connection and interaction shall necessarily originate from its own secured network domain • The audio-visual interaction shall be triggered from company own domain and not from third party service domain. • The recorded video shall be stored in safe and secure custody with date and time stamp. The technology outsourcing for V-CIP shall be covered by RBI guidelines applicable and issued from time to time.
15	Data Encryption	• The V-CIP system shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. • The customer consent should be recorded in an auditable and alteration proof manner
16	Control On IP	• The V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.
17	System Testing	• The V-CIP system shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. • The test certificate shall be recorded and kept for future reference from competent authority.
18	Audit Trail	• The activity log along with the credentials of the official performing the V-CIP shall be recorded and preserved.
19	Clear Workflow	• To carry out V-CIP a clear laid down workflow to be documented which incorporates all regulatory requirements.
20	Reporting of Fraud under RBI Guidelines	• Any case of forged identity through V-CIP shall be reported as a cyber security event under extant regulatory guidelines.

21	Employee Training	• All the employee who will engage in executing V-CIP and doing concurrent audit shall be trained by department owning the V-CIP. • The employee should be capable to carry out liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it. • Any prompting, observed by employee at end of customer end shall lead to rejection.
22	V-CIP Failure	• If there is a disruption in the V-CIP procedure, the same should be aborted and a fresh session to be initiated. • Due to any reason if V-CIP fails or becomes negative, the normal physical process of customer identification process shall be open of execution. • The V-CIP executing employee or concurrent auditor shall record the reason for failure of V-CIP if stage is reached in V-CIP. There can be some technical reason for failure or non-execution of V-CIP.
23	V-CIP Data and Video Storage	• The entire data and recordings of V-CIP shall be stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search.

5.2.4 – Digital KYC

Digital KYC means the capturing live photo of the customer and OVD/proof of possession of Aadhaar, where offline verification cannot be done, along with latitude and longitude of the location where such live photo is being taken by the company employee. The perquisite norms to execute the facility of Digital KYC:

1. The company required to have Digital Application to execute digital KYC process with customer.
2. The access of the Application shall be controlled by the company and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by company to its authorized officials.
3. The customer, for the purpose of KYC, shall visit the location of the authorized officer of the company or vice-versa. The original OVD shall be in possession of the customer.
4. The company must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the company shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by company) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.
5. The Application of the company shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white color and no other person shall come into the frame while capturing the live photograph of the customer.
6. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and watermarking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.
7. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.
8. Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.

9. Once the above-mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officers registered with the company shall not be used for customer signature. The RE must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.
10. The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the company. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.
11. Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the company, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to customer for future reference.
12. The authorized officer of the company shall check and verify that:
    (i) information available in the picture of document is matching with the information entered by authorized officer in CAF.
    (ii) live photograph of the customer matches with the photo available in the document; and (iii) all of the necessary details in CAF including mandatory field are filled properly;
13. On Successful verification, the CAF shall be digitally signed by authorized officer of the company who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.

5.2.5 CKYCR

CKYCR is an entity under CERSAI to receive, store, safeguard and retrieve the KYC records in digital form of a customer. CKYCR manages the KYC for Individual and Legal Entities.

Sharing of information to CKYCR

- Operations to upload KYC record of customer within 10 days of commencement of an account-based relation such as booking of the contract.
- Applicable operational guideline issued by CERSAI for uploading the KYC data shall be followed.
- The KYC of Individual and Legal Entities to be uploaded with CKYCR of the accounts opened on or after 01.04.2017 and 01.04.2021 respectively.
- The KYC Identifier generated by CKYCR to be informed to Individual and Legal Entity as the case may be.
- The CKYCR identifier generated after submission of KYC is required to be communicated to the respective customer.
- Period updation of the KYC information / documents received for Individual and Legal Entities to be done for prior to and after the above-mentioned dates.
- During periodic updation the customers are migrated to current CDD standards (KYC documentation and information).

Use of Information from CKYCR

- With an explicit customer consent and submission of KYC Identifier from customer or with the help of acceptable digital solutions, the company shall retrieve the KYC records online/download from CKYCR

using KYC Identifier. In such cases customer will not be required to submit KYC / OVD document or information or any other additional identification document or detail, subject to following conditions:

i. This provision is applicable only for customers falling under Low Risk or Medium Risk category.
ii. That there is no change in information (such as identification detail, Address, other personal information) of the customer as existed in CKYCR, and
iii. Address as per application form and CKYC documents is same. Additionally, wherever FI is done, FI should confirm the same address.
iv. Acceptable vintage of CKYC document used shall be defined by Risk Department from time to time.
v. The document should be valid at the time of proposed loan and it should an acceptable KYC document as per the Policy.
vi. If for any specified reason customer is picked up for additional/enhanced due diligence, then customer Identity and Address shall be verified through appropriate means which may include submission of additional KYC document and personal visit.
vii. In case contact point verification / customer interaction reports that customer address / KYC detail does not match with the downloaded KYC then fresh KYC shall be obtained.
viii. Additionally, in case of Non-Individual customers the following documents are required afresh from customer / digital source -
    - Company - Board Resolution, List of Directors, Latest Shareholding pattern, Power of Attorney (if applicable).
    - Partnership Firm - Partnership deed/list of partners with profit sharing ratio, Partnership Authority Letter, Power of Attorney (if applicable).
    - HUF – HUF Letter.
    - AOP/BOI (including Trust, Society etc.) - list of members with beneficial interest percentage Resolution as per entity type, Power of Attorney (if applicable).

5.3. RISK MANAGEMENT

5.3.A CUSTOMER SCREENING

The risk assessment procedure begins with screening of the Negative/ Freeze lists. On receipt of any caution lists being provided by the Reserve Bank of India to the Legal/ Compliance Department, the same shall be provided by the Business Intelligence Department to the IT department for uploading in Internal Dedupe Database. The procedure for screening of lists is as follows:

(i) The Internal Dedupe database will be enhanced with various lists to screen the name, date of birth and /or relevant data of the customer,
(ii) When information of an existing customer or the Beneficial Owner of an existing account, subsequently becoming a PEP is obtained either from information available in public domain or customer interaction at branch or during servicing of accounts, senior management approval would be required to continue the business relationship and the account shall be subject to enhanced CDD measures.
*-Politically exposed persons are individuals who are or have been entrusted with prominent public functions by a foreign country, including the Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations, important political party officials, etc.

DFSPL will not allow opening and/or holding of an account on behalf of a client/s by professional intermediaries, like Lawyers and Chartered Accountants, etc., who are unable to disclose true identity of the owner of the account/funds due to any professional obligation of customer confidentiality. Further, any professional intermediary who is under any obligation that inhibits DFSPL ability to know and verify the true identity of the client on whose behalf the account is held or Beneficial Ownership of the account or understand true nature and purpose of transaction/s, should not be allowed to open an account on behalf of a client.
It should be also noted that information collected from the customer for the purpose of opening of account should be kept confidential and not divulged for cross selling or any other purpose. Any other information if required from the customer shall be sought separately.

5.3.B CUSTOMER RISK CATOGRIZATION

Risk Profile
As per the Company's "Know Your Customer (KYC) and Anti Money Laundering Measure" policy customer will be categorized into Low Risk, Medium Risk, High Risk and Unacceptable based on the risk profile of the customer.

Process of Risk Profiling
For Risk management, the Company has a Risk based approach, after taking into consideration the assessment and risk perception of the Company. Each customer is categorized into low, medium and high risk. In this note, the term "risk" is considered in the context of money laundering and financing terrorism (not credit risk, loan default risk, etc.). \

Risk profiling of customer is based on customer's identity, social/financial status, nature of business activity, information about the customer business and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

5.4 CUSTOMER DUE DILIGENCE (CDD) MEASURES
CDD measures are applied based on the risk profile of the customer. The risk ratings and the related due diligence measures are summarized below:

Risk Profile	**Due diligence Measures**
Low & Medium risk	Standard Measures
High risk	Enhanced Measures

5.4.A Process for Customer Risk Categorization:

1. Relevant section specifying the Risk Category of the customer should be filled in
2. Risk categorization of customers into Low (Category A), Medium (Category B) & High Risk (Category C) shall be done based on information available.
3. For customers categorized as "High risk (Category C), enhanced due diligence as specified below is mandatory:
   (a) DFSPL Group Employee to visit the customer's premises to ascertain the real existence of such a business/industrial unit/financial status person and its scale of operations commensurate with its turnover.

(b) Case needs to be approved post recommendation from Head of Business by Head Credit/National Credit Manager and Risk Head/Chief Risk Officer jointly after review of customer visit report, financial documents & source of funds.
(c) Operations shall ensure that no disbursement is made unless the Risk Categorization is done.
(d) Operations shall also ensure that the respective approvals for customers classified as High-Risk customer are available.
(e) Operations to also ensure that correct risk categorization is updated in SAP.

4. It is to be noted that the customer profile will be a confidential document and details contained therein shall not be divulged for any other purposes. Adequate care should also be taken by the branch functionaries to seek only such information from the customer, which is relevant to the risk category and is not intrusive.

The Company has adopted the following classification for risk categorizations of its customers.

5.4.B Definition of Customer Risk: 'Customer risk ' in the present context refers to the money laundering risk associated with a particular customer from a Company's perspective.

5.4.B.1 High Risk Customers (Category C):
Characteristics of High-Risk Customer: Customers whose source of funds are not clear or are not convincing will be categorized as High Risk customer. Higher due diligence shall be applied for this category of customers.
Indicative List:

- Multi-level Marketing firms
- Customer reported to FIU under Suspicious transaction reporting/cash transaction reporting as per PMLA norms.

5.4.B.2 Medium Risk Customers (Category B):
Characteristics of Medium Risk Customer: Customers that are likely to pose a higher than average risk to the Company may be categorized as medium risk customer.
Indicative List:

- Trusts / Societies who do not maintain books of accounts other than Educational Trust/society, charities, NGO's and Organization receiving donations.
- Politically Exposed Persons (PEPs) as per RBI.

5.4.B.3 Low Risk Customers (Category A):
Characteristics of Low Risk Customer: Individuals and entities whose identities and source of wealth can easily identifiable and transactions in whose accounts by and large conform to the known profile will come under this category. Customers not Covered in the High Risk and Medium Risk category definition will be categorized as low risk customer.

Indicative List:

- Profiles engaged in transportation/related activities.
- Salaried Employees/Pensioners/Self Employed profiles

- All entities with Income documents like Balance sheet, P&L, Bank Statement and other documents from which source of income/capital can be easily ascertained.
- Profiles which are not specified under High Risk or Medium Risk.

5.4.B.4 Unacceptable Customers:

Customers that are likely to pose a highest risk to us may be categorized Unacceptable Customers, such as:

- Match against the Terrorist list, RBI watch list & Country list ((indicative list provided by IBA and United Nations) in Dedupe check.
- Lending to Private Finance companies not registered with RBI.

5.4.B.5 For existing customers:

- In the event of any change in the risk profiling, the latest risk profiling will prevail.
- Customer reported to FIU under Suspicious transaction reporting/cash transaction reporting as per PMLA norms to be classified as high risk customer if earlier classification is different.

5.4.B.6 Updation of negative database:

The Company through its department of Compliance, Business Intelligence & Analytics (BIA) and IT shall ensure the de-dupe data base is updated at specified interval from the negative data source as mentioned below:

Terrorist List periodically circulated by United Nations Security Council (UNSC).
The details of the two lists are as under:

i. The "ISIL (Da'esh) &Al-Qaida Sanctions List", which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL &Al-Qaida Sanctions List is available at
ii. https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xsl
iii. The "1988 Sanctions List", consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/taliban-r.xsl.
iv. In addition to the above, other UN Sanctions circulated by the Reserve Bank and circulated by Compliance department in respect of any other jurisdictions/ entities from time to time shall be updated by BIU & IT department for implementation of Section 51-A of Unlawful Activities Prevention Act (UAPA), 1967.

5.4.C ON-GOING DUE DILIGENCE

The Company shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds. The extent of monitoring shall be aligned with the risk category of the customer. Review of Risk Categorization Indicative list for each category shall be done once in 6 months by Risk Department.

Operations and Sales department will periodically update customer identification data after the account is opened. The periodicity (from the date of account opening/last verification of KYC) of such updation should not be less than once in ten years in case of Low Risk category customers, not less than eight years for Medium

Risk category and not less than once in two years in case of high risk categories subjected to following conditions:

(a) Fresh proofs of identity and address shall not be sought at the time of periodic updation, from customers who are categorized as 'low risk', when there is no change in status with respect to their identities and addresses and a self-certification to that effect is obtained.

(b) A certified copy of the proof of address forwarded by 'low risk' customers through mail/post, etc., in case of change of address shall be acceptable.

(c) Physical presence of customer at the time of periodic updation shall not be insisted upon. Documents for the purpose of re updation can be accepted through mail/post/courier etc.

(d) The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.

(e) Fresh photographs shall be obtained from customer for whom account was opened when they were minor, on their becoming a major.

5.4.D - Policy on Risk-Based Approach for Periodic updation of KYC Documents

Following risk-based approach for periodic updation of KYC has been adopted.
Periodic updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers from the date of opening of the account / last KYC updation.

1. Individual Customers:

a) **No change in KYC information:** In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the company, customer's mobile number registered with the company, digital channels (such as online banking / internet banking, mobile application of company), letter etc.

b) **Change in address:** In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the company, customer's mobile number registered with the company, digital channels (such as online banking / internet banking, mobile application of company), letter etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.

2. Customers other than individuals:

a) **No change in KYC information**: In case of no change in the KYC information of the legal entity customer, a self-declaration in this regard shall be obtained from the legal entity customer through its email id registered with the company, digital channels (such as online banking / internet banking, mobile application of company), letter from an official authorized by the legal entity in this regard, board resolution etc. Further, company shall ensure during this process that Beneficial Ownership (BO) information available with them is accurate and shall update the same, if required, to keep it as up to date as possible.

b) **Change in KYC information:** In case of change in KYC information, RE shall undertake the KYC process equivalent to that applicable for on boarding a new legal entity customer.

3. Additional measures: In addition to the above, company shall ensure that -

a) The KYC documents of the customer as per the current CDD standards are available with them. This is applicable even if there is no change in customer information but the documents available with the company are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the RE has expired at the time of periodic updation of KYC, company shall undertake the KYC process equivalent to that applicable for on boarding a new customer.

b) Customer's PAN details, if available with the company, is verified from the database of the issuing authority at the time of periodic updation of KYC.

c) An acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database of the company and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

d) In order to ensure customer convenience, company may consider making available the facility of periodic updation of KYC at any branch.

e) Company shall ensure that their internal KYC policy and processes on updation / periodic updation of KYC are transparent and adverse actions against the customers should be avoided, unless warranted by specific regulatory requirements.

5.5. AML PROCESS: TRANSACTION MONITORING

Ongoing monitoring is an essential element of effective KYC procedures. Effective control and reduction of risks is possible only if there is a clear understanding of the normal and reasonable activity of the customer. This would in turn enable DFSPL to identify the transactions that fall outside the regular pattern of activity. However, the extent of monitoring shall be dependent on the risk sensitivity of the account.

5.5.A Type of transactions to be monitored

Following are some types of transactions which should be closely monitored:

1. all cash transactions of the value of more than rupees Ten Lakh or its equivalent in foreign currency;
2. all series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds rupees ten lakh or its equivalent in foreign currency
3. all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place;
4. all suspicious transactions whether or not made in cash and in manner as mentioned in the Rules framed by Government of India under the Prevention of Money Laundering Act, 2002.

5.5.B *Instructions on Accepting Cash

i) It shall be ensured by every business unit that no cash of Rs.50,000/- and above is accepted from a customer without copy of PAN card. In case if the customer is not having the PAN card, duly filled and signed form no 60 shall be collected from the customer.

ii)

5.5.C INFORMATION TO BE PRESERVED

Following information in respect of above transactions have to be preserved:

1. the nature of the transactions.
2. the amount of the transaction and the currency in which it was denominated.
3. the date on which the transaction was conducted; and
4. the parties to the transaction.

5.5.D REPORTING OF TRANSACTIONS

The PMLA and the Rules framed there under have imposed an obligation on the Principal Officer to report all cash transactions and suspicious transactions to the Financial Intelligence Unit (FIU-IND). There shall be no restrictions on operations in the accounts where an STR has been made. It should be ensured that there is no tipping off to the customer at any level.

The types of transactions to be reported and the manner of reporting shall be done as detailed hereunder:

I. Reporting of Cash Transactions

The following types of transactions shall be reported to the FIU-IND:

i) All cash transactions of Rs.10 Lakhs and above or its equivalent in foreign currency;

ii) all series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds rupees ten lakh or its equivalent in foreign currency

Illustration of Integrally connected cash transaction

The following transactions have taken place in an NBFC during the month of April,2008:

Date	Mode	Dr. (in Rs.)	Cr. (in Rs.)	Balance (in Rs.) BF - 8,00,000.00
02/04/2008	Cash	5,00,000.00	3,00,000.00	6,00,000.00
07/04/2008	Cash	40,000.00	2,00,000.00	7,60,000.00
08/04/2008	Cash	4,70,000	1,00,000.00	3,90,000.00
Monthly Summation		10,10,000.00	6,00,000.00	

1. As per above clarification, the debit transactions in the above example are integrally connected cash transactions because total cash debits during the calendar month exceeds Rs.10 lakhs. However, DFSPL should report only the debit transaction taken place on 02/04 & 08/04/2008. The debit transaction dated 07/04/2008 should not be separately reported by the NBFC, which is less than Rs. 50,000/-.
2. All the credit transactions in the above example would not be treated as integrally connected, as the sum total of the credit transactions during the month does not exceed Rs.10 lakhs and hence credit transaction dated 02, 07 & 08/04/2008 should not be reported.

Time of Reporting

i) The reporting of Cash Transactions to the FIU-IND shall be made only through the Principal Officer/Company Secretary appointed by the Company.

ii) Upon the receipt of the documents referred above, the Principal Officer and the Company Secretary shall report the Cash Transaction/s referred to in above Para) to the Director, FIU-IND immediately not later than

15th of the succeeding month to which the transaction relates while doing so individual transactions below rupees fifty thousand may not be included.
iii) This reporting shall be done in the format prescribed.
iv) Utmost confidentiality should be maintained in filing of CTR with FIU-IND.

II. Reporting of Suspicious Transaction

Suspicious transaction means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or

b. appears to be made in circumstances of unusual or unjustified complexity; or

c. appears to not have economic rationale or *bona-fide* purpose; or

d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

Apart from reporting Cash transactions of the above nature, the Principal Officer and the Company Secretary is also under an obligation to report all transactions of a suspicious nature to the Director, FIU-IND. STRs should be made if there are ground to believe that the transaction involves proceeds of crime generally irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.

While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. The company shall not put any restriction on operations in the accounts where an STR has been filed. The company shall keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level.

Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

Indicative List of Suspicious Activities

1. Transactions Involving Large Amounts of Cash:
   Company transactions, that are denominated by unusually large amounts of cash rather than cheques / Electronic payments etc.
2. Transactions that do not make Economic Sense:
   Transactions in which assets are withdrawn immediately after being deposited without adequate justification.
3. Activities not consistent with the Customer's Business:
   Accounts with large volume of credits whereas the nature of business does not justify such credits.

4. Attempts to avoid Reporting/Record-keeping Requirements
   A customer who is reluctant to provide information needed for a mandatory report
   Any individual or group that coerces/induces or attempts to coerce/induce a DFSPL employee not to file any reports or any other forms.
5. An account where there are several cash transactions below a specified threshold level to avoid filing of reports.
6. Unusual Activities
   Funds coming from the countries/centers which are known for money laundering.
7. Customer who provides Insufficient or Suspicious Information
   a. customer/company who is reluctant to provide complete information regarding the purpose of the business, prior business relationships, officers or directors, or its locations.
   b. A customer/company who is reluctant to reveal details about its activities or to provide financial statements.
   c. A customer who has no record of past or present employment but makes frequent large transactions.
8. Certain Employees arousing Suspicion
   a. An employee whose lavish lifestyle cannot be supported by his or her salary.
   b. Negligence of employees/willful blindness is reported repeatedly.
9. Some examples of suspicious activities/transactions to be monitored by the operating staff-
   a. Large Cash Transactions
   b. Multiple accounts under the same name
   c. Placing funds in term Deposits and using them as security for more loans
   d. Sudden surge in activity level
   e. Same funds being moved repeatedly among several accounts

Please Note: This is not an exhaustive list but is merely an indicative list.

Time of Reporting

i) The reporting of Suspicious Transactions to the FIU-IND shall be made only by the Principal Officer/Company Secretary appointed by the Company.

ii) Upon receipt of the above referred annexures the Principal Officer/ Company Secretary shall report the Suspicious Transaction/s to the Director, FIU-IND within 7 days from arriving at a conclusion that a Suspicious Transaction has taken place.

iii) This reporting shall be done in the format prescribed by FIU-IND.

iv) The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or any other office. Such report shall be made available to the competent authorities on request.

v) It should be further noted that, Suspicious Transaction Reports shall also be filed if there are reasonable ground to believe that the transaction involves proceeds of crime generally irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.

vi) Utmost confidentiality should be maintained in filing of STR with FIU-IND.

5.5.E REPORTING OF FORGED OR COUNTERFEIT CURRENCY

NOTES OR BANK NOTES

All cash transactions where forged or counterfeit Indian currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place shall be reported to the Principal Officer/ Company Secretary in the manner prescribed hereunder.

Time of Reporting

i) The reporting of the above referred transactions to the FIU-IND shall be made only through the Principal Officer/Company Secretary appointed by the Company.

ii) Upon the receipt of the CCR, the Principal Officer/Company Secretary shall report the said transaction/s to the Director, FIU-IND by the 15th day of the succeeding month of occurrence of such transaction in the format prescribed for Summary Counterfeit Currency Report (CCR). The delay in reporting such transaction shall be construed as non-compliance.

Record keeping

Central Operations (COPS) shall be responsible for record keeping and retention of all documents as per the PMLA, 2002 Rules. Records of all transactions shall be maintained for a period of 5 years from the date of transaction between the customer and the DFSPL. The documents are to be preserved in a hard copy/ digitized manner (as may be intimated) so as to enable reconstruction of individual transactions (including the types and currency of transaction involved, if any) and provide, if necessary, evidence for prosecution of persons involved in criminal activity.

Records pertaining to the identification of the customer and his / her address (e.g. copies of documents like passports, identity cards, driving licenses, PAN, utility bills etc.) obtained while opening the account and during the course of business relationship, would be properly preserved as mentioned above for at least 5 years after the business relationship is ended.

The following types of transactions are to be recorded and reported in the manner provided under the Reporting section of this policy:

i) all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;

ii) all series of cash transactions (pertaining to one customer or link account i.e. code and Group code in SAP / BANCs**)** integrally connected to each other which have been valued below rupees ten lakh or its equivalent in foreign currency, where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds rupees ten lakh;

iii) all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place;

iv) all suspicious transactions whether or not made in cash and in manner as mentioned in the Rules framed by Government of India under the Prevention of Money Laundering Act, 2002.

5.5.F – Policy on Money Laundering & Terrorist Financing Risk Assessment

In order to have constant check over the risk posed due to money laundering and terrorist funding, Risk Assessment would be conducted by the Internal Audit Department (IAD).

i) IAD shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.
ii) The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal

risk assessment, the Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with the Company from time to time.

iii) The risk assessment by the Company shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company. Further, the periodicity of risk assessment exercise shall be determined by the Board of the company, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

iv) The outcome of the assessment shall be put up to the Board or any committee of the Board to which power in this regard has been delegated and should be available to competent authorities and self-regulating bodies.

v) The suggestion and mitigants confirmed by Board shall be implemented. IAD shall monitor the implementation of the controls and enhance them if necessary. Company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard. Further, company shall monitor the implementation of the controls and enhance them if necessary.

vi) IAD would decide suitable process / procedural aspects by Chief Internal Auditor based on the above guidelines to implement the same.

5.6 BUSINESS PARTNER DUE DILIGENCE PROCEDURE

5.6.A BUSINESS PARTNER DUE DILIGENCE (BPDD)

Definition

A Business Partner is defined as "any party who establishes relationships on behalf of their clients with DFSPL and parties whose employees have access to DFSPL's data and or systems (outsourcing partners, providers of administrative / IT services, External auditors, data entry operators, Consultancy firms etc.)" The Outsourcing Policy of DFSPL governs all Business Partner relationships.

KYC Policy including Risk Categorization will be applicable to all Business Partners including associates / agencies / intermediaries etc.:

- Empaneled Lawyers - Empaneled Valuers - Vendors providing services like Selling Agents, Direct selling team / agents, Collection Agencies, Verification Agencies, Bidders etc. –
- Any other intermediary.

DFSPL will collect all KYC documents as specified in Annexures.

Due- diligence of Business Partners:

The Business Partner relationships are entered into at the Corporate Office /Regional Office/Head office level. Hence the Heads of Business Units/Departments are responsible to ensure adequate due diligence measures are applied before accepting a Business partner. Following procedure to be followed:

Step 1

Heads of Business Units/Departments should collect information of the following parties as part of the due diligence:

(i) The Business Partner as a person as such as defined above.

(ii) Individuals who are authorized to act on behalf of the business partner.

(iii) The Beneficial Owner (BO) of the business partner,

Step 2

The Heads of Business Units/Departments should screen the names and date of birth/other relevant date of the Business Partner and its BO/Representatives against the freeze /negative lists / Dedup database. In case of hit on the lists screened, enhanced measures should be applied to ascertain the identity of the Business Partner. The enhanced measures are same as the enhanced measures for Customer Acceptance.

Step 3

A pre-employment screening of the staff of the business partners who have /may have access to DFSPL's data or systems should be performed.

Review of Business Partners:

Periodicity

The Business Partner files have to be reviewed with every material change that comes to the notice of DFSPL. Records of business partners should be reviewed every year by Sales and Operations.

Step 1

The Business / Department that has performed the due diligence on accepting the Business Partner is also responsible for periodical review. Audit department shall monitor and ensure all the Business / Department comply with this procedure and perform timely reviews.

Step 2

The review should be performed using the due diligence form for Business Partners. The revised due diligence forms should be kept along with the Agreement.

5.7 ANNEXURES

Annexure A1 - Documentation

Officially Valid Document (OVD): OVD means one of the following documents with OSV (physical / digital / electronic):

1. Valid Passport issued in India.
2. Valid Permanent Driving License (unexpired).
3. Aadhaar Card* (Letter issued by the Unique Identification Authority of India containing details of Name, Address and Aadhaar number).
4. Voters' Identity Card Issued by Election Commission of India.
5. Valid Job Card issued by NAREGA duly signed by Officer of State Government.
6. Letter issued by the National Population Register containing details of name and address.

***** Aadhaar Number Validation & Redaction – Company shall, where its customer consents to submit his Aadhaar number, ensure such customer to redact or blackout his Aadhaar number through appropriate means. RBI has allowed for Offline verification in such cases.

Important points

- Where Permanent Account Number (PAN) is obtained, the same shall be verified from verification facility of the issuing authority.
- Where an equivalent e-document is obtained from the customer, company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).
- Copies of the KYC documents (physical / digital) should be verified with originals and certified by the person verifying the same as 'True Copy' i.e. Original, Seen and Verified (OSV). The DFSPL Group Employee or DFSPL Group Representative who meets the customer should perform the verification (OSV stamp with name, signature and employee / representative code) in physical/digital/electronic mode.
- The KYC documents scanned/uploaded in digital/electronic mode shall be stored in system and it should be available for reference as and when required. In such cases, physical copy may not be stored.
- KYC documents of Beneficial Owner (BO) has to be mandatorily collected. BO is defined as per Annexure A2.
- KYC documents issued in incomplete names (only personal names (first names) as in the case of Voter ID in certain states) cannot be accepted.
- KYC documents collected for address proof should contain the complete address as captured in the application form. If there is any difference or if the details are incomplete (as per manual check or rule engine based system check), then another document containing the address as per application form should be taken.
- Marriage Certificate issued by state govt. or gazette notification to be used in case of name change along with certified copy of KYC documents in existing name to be obtained for identity and address proof of the person and can be used for relationship proof.
- In case of a partnership between individual(s) and entity(s) or between entity(s), the KYC requirements for such entity(s) also need to be complied with in addition to the KYC requirements of the partnership.
- KYC document/information can be validated digitally through external vendors appointed by the company. Any of the following i.e. Physical or manual mode / Optical Character Recognition (OCR) / Digital Scanning can be used to capture the information. Information captured though OCR / Scanning and the information validated through external vendor should match as per the logics specified in system based rule engine.
- In case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), alternatively, the original certified copy of OVD, certified by any one of the following, may be obtained: Authorised officials of overseas branches of Scheduled Commercial Banks registered in India, Branches of overseas banks with whom Indian banks have relationships, Notary Public abroad, Court Magistrate, Judge, or Indian Embassy/Consulate General in the country where the non-resident customer resides.
- Where OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

KYC DOCUMENTATION

Customer Type	Documents
Individual	The Company shall obtain the following from an individual (applicant, co-applicant, guarantor) while establishing an account-based relationship or while dealing with the individual who is a

Customer Type	Documents
	Beneficial Owner, authorised signatory or the power of attorney holder related to any legal entity or customer/transaction as defined in 'Applicability Section': 1. Recent color passport size photograph (Physical / digital / Selfie) 2. Permanent Account No. issued by Income Tax Authority (mandatory) 3. Aadhaar Card (Letter issued by the Unique Identification Authority of India containing details of Name, Address and Aadhaar number). Aadhaar may be taken with Offline Verification of a customer if he is desirous of undergoing the same and the address in Aadhaar is updated (i.e. same as per application form where customer is residing currently). • Alternatively, any one of the other valid OVDs with updated address shall be taken. If still the OVD furnished by the customer does not have the updated address, then any of the following additional documents with updated address shall be taken for the purpose of proof of address: (a) Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); (b) Property or Municipal tax receipt; (c) Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; (d) Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation; Where the Permanent Account Number is not available, the individual applicant shall submit Form 60, also one of the OVDs as mentioned above would be required for Identity Proof.
Proprietor ship	• Documents in the name of proprietor (Individual) as mentioned in "Individual" Section ab details of identity and address of the individual (proprietor) and • In addition to the above, any two of the following documents as a proof of business / activity in the name of the proprietary firm shall also be obtained: (a) Registration certificate (b) Certificate/licence issued by the municipal authorities under Shop and Establishment Act. (c) Sales and income tax returns. (d) CST/VAT/ GST certificate (provisional/final) (e) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities. (f) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. (g) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities. (h) Utility bills such as electricity, water, landline telephone bills, etc. In cases where DFSPL is satisfied that it is not possible to furnish 2 such documents then one of the above documents can be accepted Subject to contact point verification by DFSPL employee / BDM OR CPV is done by CPV Agencies to collect all such information as would be required to establish the existence of such firm, confirm, clarify and satisfy themselves that the business

Customer Type	Documents
	activity has been verified from the address of the proprietorship Firm.In instances where CPV is not done by DFSPL employee, Tele-verification by DFSPL Employee needs to be mandatorily documented in the file.
Registered Partnership firms	One certified copy of each of the following documents or equivalent e-documents shall be obtained: 1. Registration certificate, 2. Copy of Partnership Deed (partnership deed should contain a provision for borrowing clause covering hypothecation / creating charge on the asset belonging to the firm and giving guarantee) executed on stamp paper or franked and signed by all partners at least on last page under authority stamp (for capacity) 3. Partnership Authority Letter (PAL): All pages of the Partnership letter to be signed by minimum one partner. All Partners should sign and authenticate at least last page of the PAL under rubber seal (for capacity). The PAL should be on the Firm's Letterhead. Any alterations on any page to be signed by all the partners. 4. Copy of PAN Card in the name of partnership firm 5. Documents as specified in Individual section for the partner, BO, authorized signatories and individual holding an attorney to transact on firm's behalf.
Public Limited / Private Limited companies	One certified copy of each of the following documents or equivalent e-documents shall be obtained: 1. Board Resolution to apply and avail the loan and power of attorney granted to its managers, officers or employees to transact on its behalf. 2. Certified True copy of Board Resolution from the Company Secretary/Managing Director to the effect that the person signing the loan document has the authority to execute the deal on behalf of the company along with the extract of the Board Resolution in this respect. 3. Latest List of all Directors with their addresses signed and dated by the Company Secretary / Director(s)so as to ensure the certifying Director name is in the List of Directors submitted by the Company. Refer Annexure A4 in case of change of directorship. 4. Copy of PAN Card in the name of company, 5. Copy of Certificate of incorporation (COI), Memorandum of Association (MOA), Articles of Association (AOA) verified with original. Copy of certificate of commencement of business in case of public limited companies. The AOA should permit the company to borrow and give a guarantee. 6. Documents as applicable for individuals, Authorized Signatories and BO as specified in "Individuals" Section. 7. Certified Information to be collected about the shareholding/ownership share/profit share/beneficiary for establishing percentage holding
Trust/Association / Society/Club / Universities - Registered	One certified copy of each of the following documents or equivalent e-documents shall be obtained: 1. Registration Certificate. 2. Copy of PAN in the name of entity. 3. Certified "True and updated" copy of Trust Deed / Bye Laws / MOA attested by Secretary/ Managing Trustee/ Chairperson. 4. Certified " True and Updated" Copy of Certificate of Registration (For Club / Society / Association/ Trust) signed by the secretary. 5. List of all Office Bearers / Trustees, along with Settlers (including any person settling assets into the Trust), grantors, protectors, beneficiaries (when they are defined) and in

Customer Type	Documents
	case of Foundations the founders / managers / directors, to be obtained on the letterhead with their addresses. 6. Certified copy of Resolution to borrow facility / loan signed by managing trustee/chairperson/ secretary. 7. Documents of Trustee, BO and authorized signatory signing the facility / loan documents as specified in "Individuals" Section above. 8. Notarized Power of Attorney granted to managers, officers or employees of the firm to transact business on its behalf, if such managers, officers or employees are entering into the contract, on behalf of the firm. Certified copy of OVD of PoA holder has to be obtained. Notarized PoA would not be required if one or more member of the Trust/Society/etc. are directly executing the contract. (Annexure A5). 9. Information to be collected about the shareholding/ownership share/profit share/beneficiary for establishing percentage holding.
Hindu Undivided Family (HUF)	One certified copy of each of the following documents shall be obtained: 1. HUF letter with specimen signatures of the Karta and all adult co-parceners as per HUF Declaration Format provided in Annexure A3. 2. PAN Card in the name of HUF. 3. Documents of Karta. (As applicable for Individuals) 4. Address proof of the HUF: a. Latest available Income Assessment order OR b. Bank statement of account with existing Banker (Scheduled Bank) bearing the account holder's address with entries of preceding 3 calendar months from the date of Log in.
Unregistered Association/Body of Individual, Unregistered trusts, Unregistered Partnership firm, Universities, Local Bodies	One certified copy of each of the following documents or equivalent e-documents shall be obtained: 1. Resolution of the managing body of such association or body of individuals (PAL will be applicable for partnership firm) 2. Copy of PAN in the name of entity. 3. Certified "True and updated" copy of Trust Deed / Bye Laws / MOA attested by Secretary/ Managing Trustee/ Chairperson. 4. Partnership Authority Letter (PAL): All pages of the Partnership letter to be signed by minimum one partner. All Partners should sign and authenticate at least last page of the PAL under rubber seal (for capacity). The PAL should be on the Firm's Letterhead. Any alterations on any page to be signed by all the partners. Certified copy of OVD in respect of the person holding a PAL to transact on its behalf. 5. Notarized Power of Attorney granted to managers, officers or employees of the firm to transact business on its behalf, if such managers, officers or employees are entering into the contract, on behalf of the firm. Certified copy of OVD of PoA holder has to be obtained. Notarized PoA would not be required if one or more partners of the firm are directly executing the contract. (Annexure B4). 6. Proof of legal existence of such entity in the form of Service Tax/VAT/Sales Tax Registration/ CST/VAT/GST certificate/ Certificate of registration document issued by Sales Tax/Service Tax/Professional Tax authorities/Udyog Aadhaar Registration Certificate. 7. Information to be collected about the shareholding/ownership share/profit share/beneficiary for establishing percentage holding. Explanation: Unregistered trusts/partnership firms shall be included under the term 'unincorporated association'. Explanation: Term 'body of individuals' includes societies.

Annexure A2

Process of determination of BO:

1. Where the client is a person other than an individual or trust:
    a. BO is the person exercising control through ownership interest.
    Where the Non individual client is-

        i. **Company:**
            1. Person having ownership of/entitlement to more than 10 percent of shares or capital or profits of the said Company or
            2. A person having the right to appoint a majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders' agreements or voting agreements shall be the BO of the company.
        ii. **Partnership Firm:** Person having ownership of/entitlement to more than 10% of the capital or profits of the partnership firm shall be the BO
        iii. **Unincorporated association or body of individuals:** Person having ownership of/entitlement to more than 15% of the property or capital or profits of the unincorporated association or body of individuals shall be the BO

    b. Where no natural person exerts control through ownership interests, BO shall be the person exercising control over the non-individual client through other means like control over voting rights, agreements, arrangements etc.

    c. Where no natural person is identified under (a) or (b) above, BO shall be the person who holds the position of senior managing official of the non-individual client.

2. Where the client is a trust: BO shall be-
    a. Author of the trust, the trustee, the beneficiaries with 15% or more interest in the trust
    b. Any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

3. Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or Beneficial Owner of such companies.

Annexure A3

HINDU UNDIVIDED FAMILY LETTER
Date:

To,

Dowell Fiscal Services Pvt LtdDowell Fiscal Services Pvt Ltd Ltd.
_____Branch.

Dear Sir,
The business of …… carried on in the firm name and style of…..at ……. is the ancestral business of the Joint Hindu family governed by the Mitakshara/ Dayabhaga Law of which I/we the undersigned am/are the present Karta or Managing Member(s) and we the undersigned are the present adult members. As the aforesaid joint family business by the nature thereof cannot be carried on without credit facilities, we have requested you to finance the aforesaid joint family business of the firm and to grant to the firm all or some or any of the credit facilities that may be agreed upon from time to time between the you and the Joint Hindu family firm for sums not exceeding at any one time in the aggregate sum of Rs. _____(Rupees only).
The following members viz.
1.
2.

are authorized jointly or severally to represent and sign on behalf of the said joint family business in manner as appears below and have full unrestricted authority to bind all the members of the joint family however constituted from time to time.

In the event of you acceding to our request and granting us the facility applied for financing we, the undersigned, undertake with the intention of binding not only the present members of the said joint family (both adults and minors) but also all future members thereof (both adults and minors) and all persons entitled to a share therein and ourselves personally and our respective interest in the joint family properties as well as our separate estates.

1. whenever any change occurs in the manager ship or in the nature of the said ancestral business or in the constitution of the said joint family or said ancestral business caused by the death of a co-parcener whether or not resulting in the share devolving on his widow or widows or by the birth of a co-parcener or if at any time any of us desire to give up or sever his connection with the said ancestral business or if we desire to close the said ancestral business or if any minor member of the said family attains majority to give notice thereof to us at once in writing and that

2. Until receipt of such notice by us and whether any provisions of the Partnership Act, 1932 shall apply or not you shall be entitled to regard each of us as partners in respect of all dealings or transactions with you which may be found to be outside the scope of the said ancestral business and that such dealings and transactions shall be binding on each of us as such partner and our respective estates and that

3. Notwithstanding any provisions of the said Act or any change in the membership of the said firm all acts purporting to be done on behalf of the said joint family business before you shall have received notice in manner aforesaid, shall be binding on the said joint family and its properties and on each of us and our respective estates and the liability of the said firm and of each of us and of our respective estates shall continue until all liabilities in respect of such acts shall have been discharged.

The names and dates of birth of the present minor* members of the aforesaid joint family are given below:

Yours faithfully,

_____

His personal signature here

1. Shri …….

……

Will sign on behalf of the firm as follows: Karta

2. Shri..... His personal signature here

Will sign on behalf of the firm as follows:

…….

*Particulars of the minor members of the joint family.

Name Father's name Date of birth

Annexure A4

DECLARATION CUM INDEMNITY (Confirming list of Directors)

To,

Dowell Fiscal Services Limited,

(Branch Address)

Kind Attn: _____

Dear Sir,

_____, a company, registered under _____ and having its registered office at _____(Complete office address) (hereinafter "the Company") do hereby declare and state as under:f

As on the date of this Declaration cum Indemnity the following are the directors of the

Company:

1. _____

2. _____

The Company hereby confirms that all the requisite legal formalities for appointment of the above mentioned Directors have been complied with including filing of Form 32 with the Office of Registrar of Companies.

The Company hereby confirms that the Company has applied to DFSPL for obtaining a.....(type of loan / facility) at the _____(Branch) and the Company has to submit various documents to DFSPL with respect to the application for the said account. The Company hereby states that the Company is unable to furnish to DFSPL a copy of Form 32 filed with the Office of Registrar of Companies with respect to the appointment of Mr. _____as a director on the account of the same having been misplaced / change in directors since incorporation.

The Company hereby agrees and undertakes to hold harmless and keep DFSPL fully indemnified against claims and damages which may be made in respect hereof by reason of DFSPL relying and acting upon the faith of this Declaration cum Indemnity.

The Company further agrees and undertakes to pay and make good all such losses, damages or expenses, upon demand being made, and also to comply with such requirements including furnishing or execution of such further deeds, documents or writings as DFSPL may require.

Signed and Delivered by ---------- by the hand of its authorized signatory Mr ---------- in the presence of

1.

2.

(Stamp and Seal of Company)

Place:

Date:

Annexure A5 – Format for Power of Attorney (Stamp Duty as per state Laws and to be Notarized)

SPECIFIC POWER OF ATTORNEY

Be it known to all to whom it may concern that We, _____s/o _____ aged about, residing at _____ _____; _____s/o _____ aged about, residing at _____ _____; _____s/o _____ aged about, residing at _____ _____ and _____s/o _____ aged about, residing at _____ _____, presently acting as Partners for the Partnership Firm M/s _____ bearing registration no. _____ (In case of registered Partnership Firm) having its place of business/ address at _____do hereby nominate, constitute and appoint _____s/o_____aged about _____presently a Partner, as our Attorney to do the following acts, deeds and things on all of us jointly and severally in our name in respect of the Loan _____:

1. That. we are the Partners for the Partnership firm, M/s_____.

2. That the Partnership firm is considering to avail a loan / give guarantee for loan of Rs. _____ from Dowell Fiscal Services Limited (hereinafter to be known as "DFSPL") for the purpose of _____
3. That we hereby jointly and severally appoint and authorize Mr. _____ s/o _____ aged about _____years, who is presently a Partner to do all or an/ of the above acts, or any other acts which have not been specifically mentioned herein above, and in the opinion of our attorney, ought to be done, executed or performed in respect of the said loan or any matter incidental thereto.

4. That all the acts done and documents executed by the aforesaid Partner shall bind the firm and each of us as it each of us had ourselves done such acts and executed such documents.

5. The acts, deeds and things done or got to be done by our attorney for the purpose, shall be construed as acts, deeds and things done by the firm and all of us jointly and severally. That all of us will be jointly and severally responsible for the liabilities of the said firm and DFSPL may recover its claims and dues from any or all of the partners of the firm and the estate of the deceased partners.

6. This power of Attorney supersedes all previous Power of Attorney, or any other authorization in relation to this loan.

IN WITNESS WHEREOF, We the Executants have put our hands on these presents on the date, month and year herein below mentioned in the presence of the following witnesses:

Signature of the Partner: _____
Name of the Partner : _____

Signature of the Partner: _____
Name of the Partner : _____

Signature of the Partner: _____
Name of the Partner : _____

Signature of the Partner: _____
Name of the Partner : _____

Place: _____

DATE: / / 20XX.

Witness: