



**GIC HOUSING FINANCE LTD.**

**YOUR ROAD TO A DREAM HOME**

## KYC AND AML POLICY

*Version: GICHFL/KYC AML Policy/Nov 2024/V2*



## Table of Contents

1.	Table of Contents .....	2
2.	<a href="#">Document Owner, Version Control &amp; Review Process .....</a>	<a href="#">3</a>
3.	Omnibus Clause.....	3
4.	Objective .....	4
5.	<a href="#">Applicability &amp; Effective Date.....</a>	<a href="#">4</a>
6.	Elements of KYC Policy.....	6
7.	Compliance of KYC Policy.....	6
8.	Definitions.....	6
9.	Customer Acceptance Policy.....	8
10.	Risk Management - Customer Categorization .....	8
11.	<a href="#">Customer Identification Procedure (CIP).....</a>	<a href="#">9</a>
12.	Customer Due diligence (CDD).....	10
13.	Enhanced Due Diligence (EDD) .....	11
14.	On-going Due Diligence and Periodic updation of KYC .....	12
15.	<a href="#">General Guidelines .....</a>	<a href="#">13</a>
16.	Anti-Money Laundering - Introduction.....	15
17.	Money Laundering Process.....	15
18.	Appointment of Principal Officer and Designated Director .....	16
19.	Maintenance and Preservation of records of transactions .....	16
20.	<a href="#">Monitoring and Reporting to Financial Intelligence Unit-India .....</a>	<a href="#">17</a>
21.	<a href="#">Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS).....</a>	<a href="#">19</a>
22.	Combating Financing of Terrorism .....	19
23.	Unlawful Activities Prevention Act.....	19
24.	Money Laundering and Terrorist Financing Risk Assessment.....	21
25.	Secrecy Obligations and Sharing of Information.....	22
26.	<a href="#">Recruitment &amp; Training .....</a>	<a href="#">22</a>
27.	General .....	22
28.	<a href="#">Roles and Responsibilities.....</a>	<a href="#">23</a>
29.	Annexure I – Indicative list of customers for Risk Categorization.....	24
30.	Annexure II - List of Documents to be obtained as an Identity/ Legal Existence and Address Proof .....	25
31.	<a href="#">Abbreviations.....</a>	<a href="#">31</a>

### Version History

Sr. No.	Prepared by	Approved By	Approval Date	Version Number	Periodicity of Review
1	Credit Department	BOARD	21/10/2022	V.1.0	2 year
2	Compliance Department	BOARD	08/11/2024	V.2.0	2 year

## Document Owner , Version Control & Review Process

Particulars	Details
Version Control	This KYC-AML policy dated November 2024 is the 2nd version of KYC-AML Policy of GIC Housing Finance Ltd.
Version No.	GICHFL/KYC AML Policy/Nov 2024/V11
Document owner(s)	Chief Compliance Officer – GIC Housing Finance Ltd
Process for any modification/revision	Regulatory changes: The Chief Compliance Officer (“CCO”), and the Managing Director & Chief Executive Officer (“MD & CEO”) shall have the authority to carry out changes in the KYC-AML Policy on account of regulatory developments. Such changes to the KYC-AML Policy shall be subsequently placed before the Board of Directors.  Other changes: Any changes other than Regulatory changes shall be carried out with the approval of the Board of Directors of GICHFL.

## Omnibus Clause

All extant & future master circulars/directions/guidelines/guidance notes issued by National Housing Bank (NHB)/ Reserve Bank of India (RBI) from time to time would be the directing force for the KYC AML Policy of GICHFL and will super cede the contents of this KYC AML Policy. This includes the following circulars:

Circular Ref. No.	Circular/ Act	Issue Date
DBR.AML.BC.No.81/14.01.001/2015-16	Master Direction - Know Your Customer (KYC) Direction, 2016 as amended from time to time	February 25, 2016
NBFC (HFC).CC.No.111/03.10.136/2019-20	Extending Master Direction – Know Your Customer (KYC) Direction, 2016 to Housing Finance Companies	May 19, 2020
-	Prevention of Money Laundering Act, 2002	July 1, 2005
-	Prevention of Money – Laundering (Maintenance of Records Rules), 2005 as amended from time to time	July 1, 2005

## Objective

This Know Your Customer and Anti- Money Laundering Policy (“KYC-AML Policy”) has been divided into two broad sections – Know Your Customer guidelines and Anti Money Laundering norms. This policy sets out to standardize KYC documentation across GICHFL and establish governing principles, broad guidelines, and standards to be adopted by the Company in order to protect itself from being used by any person to launder money.

The major objectives of this policy are:

- To lay standard operating procedures on KYC norms and AML requirements.
- To ensure all necessary Customer Identification Procedures (“CIP”) / Customer Due Diligence (“CDD”)/ Enhanced Due Diligence (“EDD”) measures are followed.
- To protect the Company from being used intentionally or unintentionally by criminal elements for money laundering/ fraudulent/anti-social activities.
- To enable the Company to know/understand their customers and their financial dealings better which, in turn, would help in managing the risks prudently.
- To take appropriate action, once suspicious activities is detected, and make report to designated authorities in accordance with applicable law / laid down procedures.
- To comply with applicable laws as well as norms adopted internationally with reference to Money Laundering.

## Applicability & Effective Date

This KYC – AML policy is applicable to all the businesses undertaken by GICHFL and shall be applicable for all new and existing customers of GICHFL.

This Policy has become effective from the date of its initial approval by the Board and any subsequent amendments shall become effective from the date of approval of such amendment by the Board of Directors. All employees of GICHFL are responsible for ensuring the effective implementation of this Policy.

Clarifications on any aspects of this Policy shall be obtained from the Compliance Team.

# KNOW YOUR CUSTOMER POLICY

## Elements of KYC Policy

The KYC policy includes following four key elements:

- a. Customer Acceptance Policy
- b. Risk Management
- c. Customer Identification Procedures (CIP); and
- d. Monitoring of Transactions

## Compliance of KYC Policy

GICHFL shall ensure compliance of KYC-AML policy through:

- Senior Management Team for the purpose of KYC compliance\*\*
- Independent evaluation of the compliance to the KYC-AML policy
- Concurrent/internal audit system to verify the compliance with KYC/AML policies and procedures.
- Submission of quarterly audit notes and compliance to the Audit Committee

\*\*At GICHFL “Senior Management Team” comprises of the Managing Director/ Chief Executive Officer, Chief Compliance Officer,

GICHFL shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

## Definitions

The terms used and not defined in this Policy shall have the same meaning as assigned to them in the Reserve Bank of India (Know Your Customer (KYC)) Directions, 2016, as amended from time to time.

1. “Act” and “Rules” means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.
2. “Authentication”, in the context of Aadhaar authentication, means the process as defined under sub-section(c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, as amended from time to time.
3. Beneficial Ownership (“BO”):
  - a. Where the customer is a Company, the BO would be the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.  
Explanation: “Controlling ownership interest,” means ownership of/entitlement to more than 10 percent Of the shares or capital or profits of the company.  
Explanation 2: “Control” shall include the right to appoint 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.
  - b. Where the customer is a partnership firm, the BO is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10 percent of capital or profits of the partnership.

Where the customer is an unincorporated association or body of individuals, the BO is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 percent of the property or capital or profits of the unincorporated association or body of individuals. explanation: Term 'body of individuals' includes societies. Where no natural person is identified in any of the above non-individual entities, the BO is the relevant natural person who holds the position of senior managing official.

- c. Where the customer is a Trust, the identification of BO shall include identification of the author of the trust, the trustee, the beneficiaries with 10 percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.
4. Digital KYC: means capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the Regulated Entity (RE) as per the provisions contained in the Act.
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
6. Group: The term "group" shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act,1961(43 of1961).
7. PAN shall be mandatory in all cases and it shall be verified from the verification facility of the issuing authority.
8. Officially Valid Document ("OVD"): means the passport, the driving licence, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.

Provided that:

- a. Where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.
- b. where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:
  - i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill),
  - ii. property or Municipal tax receipt,
  - iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address,
  - iv. 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, leave, and license agreements with such employers allotting official accommodation.
- c. The customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above.
- d. Where the 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.

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State

Government or Gazette notification, indicating such a change of name.

9. Politically Exposed Persons (PEPs): 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.
10. Video based Customer Identification Process (V-CIP): an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the RE by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face customer identification process.

## **Customer Acceptance Policy**

GICHFL shall ensure that:

- No customer is on boarded in anonymous or fictitious/benami name.
- No customer is on boarded where GICHFL is unable to apply appropriate Customer Due Diligence (CDD) measures as defined as in this policy, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. Such instances shall be considered for filing an STR, if necessary, when relevant CDD measures pertaining to the customer could not be complied with.
- The mandatory information to be sought for KYC purpose while opening an account and during periodic updation is specified.
- Additional information is obtained with the explicit consent of the customer.
- A Unique Customer Identification Code (UCIC) shall be allotted while entering into new relationships with customers (individual as well as non-individuals) as also the existing customers. CDD Procedure is followed at UCIC level for all the customers including borrowers, co-borrowers, guarantors, beneficial owners. If an existing KYC compliant customer of GICHFL desires to avail another financial product of GICHFL, no fresh KYC needs to be done for such Customer, provided such Customer is an existing Customer of GICHFL as on the date of availing the fresh facility, viz. the previous loan facility is in force and subsisting. However, in such cases it must be ensured that all the KYC details of the customer are available in the respective Customer files and other necessary due diligence, wherever required, is carried out.
- Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.
- Suitable system is to put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists.
- Permanent Account Number (PAN) shall be verified from the NSDL verification facility.
- Where an equivalent e-document is obtained from the customer, GICHFL shall verify the digital signature as per the provisions of the Information Technology Act, 2000.
- Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.

Where, GICHFL forms a suspicion of money laundering or terrorist financing, and reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file a suspicious transaction report ("STR") with FIU-IND.

## **Risk Management – Customer Categorization**

Customers shall be categorized based on their KYC risk assessment and risk perception of GICHFL. Broad



principles have been laid down below for KYC risk-categorization of customers. The risk categorization of a customer and the specific reasons for such categorization shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

GICHFL may prepare a profile for each new customer based on their KYC risk categorization. The customer profile may contain information relating to the customer's identity, social/financial status, nature of business activity, information about his clients' business and their location, geographical risk covering customers as well as transactions, etc.

The nature and extent of due diligence will depend on the risk perceived by the GICHFL. However, while preparing customer profile GICHFL should take care to seek only such information from the customer which is relevant to the risk category and is not intrusive and is in conformity with the guidelines issued by NHB/ RBI in this regard. Any other Information from the customer will be sought separately with his/her consent. 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.

### Risk Category

GICHFL will classify its customers based on the below mentioned risk categories as defined by NHB/RBI from time to time. The indicative list of High Risk and Medium Risk customers is provided in Annexure I.

1. Low Risk
2. Medium Risk
3. High Risk

Note\* It is important to note that the adoption of Customer Categorization and its implementation should not become too restrictive and must not result in denial of GICHFL's services to public, especially to those, who are financially or socially disadvantaged. For ensuring the same, risk categorization of the customer would be approved by case approving authority and authorities can be modified/ further delegated by the Chief Credit Officer – GICHFL / Business Heads - GICHFL / Chief Risk officer from time to time, as may be deemed necessary.

## **Customer Identification Process (CIP)**

The CIP shall be undertaken in the following cases:

- a. At the time of commencement of an account(lending)-based relationship with the customer.
- b. When there is a doubt about the authenticity or adequacy of the customer identification data

For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, GICHFL, may 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 immediately from the third party or from the Central KYC Records Registry.
- b. Adequate steps are taken by GICHFL 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.

The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as

applicable, will be with GICHFL.

## Customer Due Diligence (CDD)

Customer Due Diligence (CDD) means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.

CDD process is applicable for selling of GICHFL's core products as well as while selling any third-party product as an Agent.

### Type of documents

Documents to be collected from the applicant / co-applicant / guarantor / any other party to the loan are as follows:

### KYC and other documents -

- Application form with live photograph/ official stamp in case of legal entity
- Officially Valid Document ("OVD")
- Signature verification (Individual)
- Any other document as specified / defined in the Product Program for various individual/ non- individual entities from time to time and approved by the Product Approval Committee.

Entity specific documents for Proprietor / Partnership / HUF/ Club/Trust / Societies / Unincorporated association or a body of individuals/ Limited Companies are:

- Proof of legal existence
- Proof of operating address
- Proof of registered address if different than operating address
- Signature verification of the authorised signatory of the entity Refer Annexure II for the list of documents and manner of Verification

### Modes of undertaking CDD:

GICHFL shall obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity:

- a. the Aadhaar number where the individual decides to submit his Aadhaar number voluntarily under first proviso to sub-section (1) of section 11A of the PML Act. In such instances, GICHFL shall carry out authentication of the individual's Aadhaar number using e-KYC authentication facility provided by the UIDAI. Further, in such a case, if the individual wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he / she may submit a self- declaration to that effect; or
- b. the proof of possession of Aadhaar number where offline verification can be carried out; GICHFL shall carry out offline verification of Aadhaar. If offline verification cannot be carried out, the customer shall submit any other OVD or the equivalent e-document thereof containing the details of his identity and address carry out verification through digital KYC as prescribed under the RBI Directions or
- c. where equivalent e-document of any OVD is obtained, GICHFL shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo or
- d. the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and
- e. such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required.

- f. V-CIP process as prescribed under the KYC Master Directions from time to time, may also be carried out as part of customer identification process, if deemed appropriate.

## Enhanced Due Diligence (EDD)

### EDD in case of Non-face-to-face customer onboarding:

Non-face-to-face onboarding would include customer onboarding without meeting the customer physically or through V-CIP. Non-face-to-face would include use of digital channels such as CKYCR, DigiLocker, equivalent e-Document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs, where there is no physical interaction with the customer.

### **Following EDD measures shall be undertaken by GICHFL for non-face-to-face customer onboarding.**

1. V-CIP shall be provided as the first option to the customer for remote onboarding.
2. In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening.
3. Apart from obtaining the current address proof, GICHFL shall verify the current address through positive confirmation such as address verification letter, contact point verification, deliverables, etc. before disbursement of the loan.
4. PAN shall be mandatory in such cases and it shall be verified from the verification facility of the issuing authority.
5. GICHFL shall ensure that the first payment is effected through the customer's KYC-complied account.
6. Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to- face manner or through V-CIP.

### Accounts of Politically Exposed Persons (PEPs):

GICHFL may establish a relationship with PEPs either as customers or as Beneficial Owners provided that apart from performing normal customer due diligence:

- Sufficient information including information about the sources of funds/ wealth, accounts of family members and close relatives is gathered on the PEP.
- The identity of the person shall have been verified before accepting the PEP as a customer.
- For any lending/ business relationship with PEP or with family members or close associates of PEP, formal approval from the Chief Compliance Officer OR Chief Risk Officer – GICHFL has been obtained.
- All such accounts are subjected to enhanced monitoring on an on-going basis.
- In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, approval from Chief Compliance Officer OR Chief Risk Officer -GICHFL will be obtained to continue the business relationship.
- All PEP accounts would be classified as 'High Risk' accounts and will be subject to enhanced monitoring on-going basis.
- We have put in place customer screening software to derive the status of the customer if classified as PEP or not along with underlying adverse or negative media attached to PEP, if any.

## **On-going due diligence and periodic updation of KYC**

### **On-going Due Diligence**

GICHFL 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/ wealth.

Without prejudice to the generality of factors that call for close monitoring following types of transactions shall necessarily be monitored:

- a) Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
- b) Transactions which exceed the thresholds prescribed for specific categories of accounts.

For ongoing due diligence, GICHFL may consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) technologies to support effective monitoring. The extent of monitoring shall be aligned with the risk category of the customer. High risk accounts have to be subjected to more intensified monitoring.

A system of periodic review of risk categorization of accounts at least once in six months, and the need for applying enhanced due diligence measures shall be put in place. GICHFL shall ensure to provide acknowledgment with date of having performed KYC updation. The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.

### **Periodic updation of KYC**

For the purpose of effective monitoring of KYC, GICHFL shall adopt a risk-based approach for periodic updation of KYC, ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high-risk. Customers identified as high-risk customers would need to submit fresh set of KYC once in 2 years, while Medium Risk Customers would need to submit fresh set of KYC once in 8 years and Low Risk Customers once in 10 years.

#### **i. 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 GICHFL, customer's mobile number registered with GICHFL, digital channels (such as mobile application of GICHFL), 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 GICHFL, customer's mobile number registered with GICHFL, digital channels (such as mobile application of GICHFL), 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 or such other methods as may be deemed appropriate. Further, GICHFL shall obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, for the purpose of proof of address, declared by the customer at the time of periodic updation.

#### **ii. Customers other than individuals (non-individual entities):**

- a) No change in KYC information:

In case of no change in the KYC information of the customer being a non-individual entity, a self-declaration in

this regard shall be obtained from the non-individual entity through its email id registered with GICHFL, digital channels (such as mobile application of GICHFL), letter from an official authorized by the non-individual entity in this regard, board resolution etc. Further, GICHFL shall ensure during this process that Beneficial Ownership information available with GICHFL is accurate and updated at the time of periodic updation.

b) Change in KYC information:

In case of change in KYC information, GICHFL shall undertake the KYC process equivalent to that applicable for on-boarding a new non-individual customer.

**iii. Additional measures to be adopted at the time of periodic updation:**

- a) The KYC documents of the customer as per the current requirements under this Policy are available. This is applicable even if there is no change in customer information but the documents available with GICHFL are not as per the current requirements. Further, in case the validity of the KYC documents available with GICHFL has expired, GICHFL shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.
- b) Customer's PAN details, wherever available, is verified from the database of the issuing authority.
- c) An acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer. Further, it shall be ensured that the information / documents obtained from the customers are promptly updated in the records / database of GICHFL and an intimation, mentioning the date of updation of KYC details, is provided to the customer.
- d) Adverse actions against the customers should be avoided, unless warranted by specific regulatory requirements.

GICHFL shall advise the customers that in compliance with the Act and Rules, in case of any update in the documents submitted to GICHFL at the time of establishment of business relationship / account-based relationship and thereafter, the customer shall submit to GICHFL the updated documents within a period of 30 days from the date of such update.

## General Guidelines

- In case an existing customer is coming for a loan again, then in such cases valid address proof should be collected only if there is any change in the current address from the address mentioned at the time of the previous loan.
- For cases wherein the Director is empowered to execute all documents on behalf of the company through Board Resolution of the company, then such Board resolution should be signed by at least two directors.
- In some cases OSV cannot be done since the property is mortgaged and the original documents are with the financier and the customer is only having photocopy of the documents. In such scenario latest income tax provisional statement is to be collected with financier's seal on the same. Address on it should match with the application form address.
- There are cases where there are mismatches in the names on the application form and the identity proof due to:
  - a) Mistake occurred/committed by the issuing authority of the ID proof.
  - b) Change of surname after marriage.
  - c) Same individual having different name mentioned in application form and KYC documents submitted (usage of title).
  - d) Elaboration of initials detailing applicant's first/ middle name & surname.

In such scenario the declaration for dual name should be obtained. The declaration should have proper affidavit. (Annexure IV)

Note – Above situations should be accepted subject to positive FI/ PD for residence and office & positive FCU.

- In case where customer has two different signatures on two different documents (as per the list given under signature proof doc) then in such case one of the signatures should match with the signature on application form.

# ANTI MONEY LAUNDERING POLICY

## Anti Money Laundering - Introduction

- 1.1. Money Laundering may be defined as cleansing of dirty money obtained from legitimate or illegitimate activities including drug trafficking, terrorism, organized crime, fraud, and many other crimes with the objective of hiding its source and rendering it in legally usable form. It is any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources. The process of money laundering involves creating a web of financial transactions to hide the origin of and true nature of these funds.
- 1.2. The general assembly of United Nations adopted the political declaration and global programme of action in 1990 in its worldwide drive against money laundering and enjoined upon member states to adopt legislation and programme against laundering on a national level. India enacted the Prevention of Money Laundering Act, 2002. (Hereinafter referred to as 'Act')
- 1.3. Money Laundering in India  
With the growing financial sector, India is vulnerable to money laundering activities. Some common sources of illegal proceeds in India are narcotics trafficking, illegal trade in gems, smuggling, corruption, and income tax evasion. Large portions of illegal proceeds are laundered through the alternative remittance system called "hawala". Under this system, individuals transfer funds from one country to another or from one state to another, often without the actual movement of currency.

### **Prevention of Money Laundering Act, 2002:**

To combat money-laundering activities, the Government of India enacted the Prevention of Money Laundering Act, 2002 ('the Act') on January 17, 2003.

The basic objective of the Act is three-fold, viz:

- To prevent, combat and control money laundering.
- To confiscate and seize the property obtained from the laundered money.
- To deal with any other issue connected with money laundering in India.

## Money Laundering Process

Money can be obtained illegally from various criminal activities like drug trafficking, terrorism, organized crime and fraud. As criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities and provide a legitimate cover for their source of income, they usually follow three stages:

- Placement – Physically disposing of cash derived from illegal activity. One way to accomplish this is by placing criminal proceeds into traditional financial institutions or non-traditional financial institutions such as currency exchanges, casinos, or check-cashing services.  
E.g. A criminal having huge crime proceeds in form of cash, can deposit this cash in bank accounts maintained with different banks, in the name of his relatives, friends and associates, in small amounts.
- Layering – Separating the proceeds of criminal activity from their source through the use of layers of financial transactions i.e., converting the proceeds of crime into another form and creating complex layers of financial transactions to hide the original source. These layers are designed to hamper the audit trail, disguise the origin of funds, and provide anonymity.



- Integration – Placing the laundered proceeds back into the economy in such a way that they re-enter the financial system as apparently legitimate funds.  
Integration means the reinvestment of those funds in an apparently legitimate business so that no suspicion of its origins remains and to give the appearance of legitimizing the proceeds.

Section 3 of the Prevention of Money Laundering Act 2002 defines the process and offences constituting money laundering. It is a charging section, and it revolves around the term “Proceeds of Crime”. If it is established that the money involved is not proceeds of crime, the person cannot be prosecuted under the Act. The term proceeds of crime have been defined under Section 2(u) of the Act as follows:

“Proceeds of crime” means any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to a scheduled offence or the value of any such property”.

The said section broadly states that if a person is involved in the process of projecting proceeds of crime as untainted property, then he shall be guilty of money laundering, for indulging in the said process the following three elements/activities shall play a very important role:

- Possession or ownership of the proceeds of crime or property acquired from proceeds of crime, which is being reflected as untainted property.
- Transactions relating to proceeds of crime like converting its form.
- Concealment of the original transaction and/or creating ghost transactions for concealing actual transactions. E.g., Possessing Benami Property, Unexplained cash credits, unexplained expenditure, bogus or fictitious accounts, unexplained investments.

Note: For details of Offences please refer Schedule II

## **Appointment of Principal Officer and Designated Director**

### **Designated Director**

The Board of GICHL has appointed Mr. Paul Lobo, Managing Director & Chief Executive Officer as “Designated Director” to ensure overall compliance with the anti-money laundering laws, regulations and policies under the PMLA Act and Rules made thereunder as amended from time to time.

### **Principal Officer**

The Board of GICHL appointed Mr. Darshit Sheth, Chief Compliance Officer as the “Principal Officer” who shall be responsible for ensuring day-to-day compliance with the anti-money laundering laws, regulations and policies.

Any change in details of the Principal Officer/ Designated Director shall be communicated to the Regulators within the timelines prescribed by them.

## **Maintenance and Preservation of records of transactions**

The company shall continue the system of maintaining proper record of transactions as required under section 12 of the PMLA read with Rule 3 of the PML Rules.





GICHFL shall take appropriate steps to evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

**Periodicity for Retention of Records:**

- i. Records of all transactions, including information relating to transactions, whether attempted or executed, the nature and value of which may be prescribed shall be maintained for a period of 8 years from the date of transaction between the Customer and the reporting entity.
- ii. Record of documents evidencing identity of its Customers and Beneficial Owners including identification data, account files, business correspondence and results of any analysis undertaken relating to its Customers shall be maintained for a period of eight years after the business relationship between a Customer and the Company has ended or the account has been closed, whichever is later.
- iii. The company will take appropriate steps to evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

**Monitoring and Reporting to Financial Intelligence Unit – India (FIU-IND)**

**Reporting of Transactions:**

The Act and the Rules have directed the Principal Officer to report all cash transactions, suspicious transactions and counterfeit transactions to the Financial Intelligence Unit (FIU-IND). The types of transactions to be reported and the manner of reporting shall be done as detailed hereunder.

**Cash Transactions Reporting (“CTR”):**

GICHFL as a matter of policy shall not accept cash or postal order from the clients. All Cash transactions amounting to Rs.5 lacs and above in a month by a single client would be monitored from an STR perspective.

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

- (i) All cash transactions of the value of Rs.10 lakh or more or its equivalent in foreign currency and above.
- (ii) All series of cash transactions integrally connected to each other which have been individually valued below Rs.10 lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds Rs. 10 lakh or its equivalent in foreign currency.
- (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.

Explanation: For determining integrally connected cash transactions, we must take into account all individual cash transactions in an account during a calendar month, where either debit or credit summation, computed separately, exceeds Rs.10 lakh during the month. However, while filing CTR, details of individual cash transactions below Rs.50,000/- may not be indicated.

The CTR for each month would be submitted to FIU-IND by 15th of the succeeding month.

**Suspicious Transactions Reporting (“STR”):**

Suspicious transaction means a transaction, including an attempted transaction, whether or not made in cash which, to a person acting in good faith -



- 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
- appears to be made in circumstances of unusual or unjustified complexity; or
- appears to have no economic rationale or bonafide purpose; or
- gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Suspicious transactions are financial transactions that one would have reasonable grounds to suspect are related to the commission of a money laundering offence, given normal business and industry practice and one's knowledge of the client.

The Company shall develop and implement appropriate methods of monitoring so that during the period of association with the customer, suspicious customer activity can be detected, appropriate action can be taken, and reports can be made if called for by government/regulatory authorities in accordance with applicable law and laid down procedures.

An assessment of suspicion should be based on a reasonable evaluation of relevant factors, including the knowledge of the customer's business, financial history, background, and behaviour.

Nevertheless, Schedule I to these guidelines enumerates specific cases of money laundering as common indicators of money laundering activity. Where there is any suspicious activity identified by any employee of the Company, the same shall be reported in the format provided in Schedule III.

- The Suspicious Transaction Report (STR) would be furnished within 7 working days of arriving at conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. GICHFL will try to ensure there is no undue delay in arriving at conclusion once a STR is received from branch/office. The Principal Officer will record reasons for treating any transaction or series of transaction suspicious in consultation with the Chief Risk Officer, Chief Credit Officer and such other officials as may be deemed necessary.
- The Principal Officer will be responsible for submission of CTR & STR to FIU-IND in formats prescribed by FIU-IND.
- While reporting confidentiality of report would be maintained and reporting will only be done in electronic form. 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.
- GICHFL may not put any restriction on operations in the accounts where STR is reported but will ensure that there is no tipping off to the customer at any level. GICHFL will report all attempted transactions of customers reported in STRs; even though transactions are incomplete and are of any amount. GICHFL shall keep the fact of furnishing of STR strictly confidential.
- GICHFL will make STRs if they have 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.
- GICHFL may consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.

## Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS):

Under FATCA and CRS, GICHFL shall adhere to the provisions of Income Tax Rules 114F, 114G, 114H and determine whether they are a Reporting Financial Institution (RFI) as defined in Income Tax Rule 114F and if so, shall take following steps for complying with the reporting requirements:

- (a) Register on the related e-filing portal of Income Tax Dept. as RFI at the link <https://incometaxindiaefiling.gov.in/> post login --> My Account --> Register as Reporting Financial Institution.
- (b) Submit online reports using digital signature of the 'Designated Director' by uploading the Form 61B or 'NIL' report, for which, the scheme of Central Board of Direct Taxes (CBDT) shall be referred to.  
Explanation – Company will refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at <http://www.fedai.org.in/RevaluationRates.aspx> for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H of Income Tax Rules.
- (c) Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H of Income Tax Rules.
- (d) Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.
- (e) Constitute a "High Level Monitoring Committee" under the Designated Director or any other equivalent functionary to ensure compliance.
- (f) Company shall ensure compliance with updated instructions/ rules/ guidance notes/Press releases/ issued on the subject by Central Board of Direct Taxes (CBDT) from time to time.

## Combating Financial Terrorism

GICHFL has developed suitable mechanism through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit – India (FIU-IND) on priority.

As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), are received from Authority, the same is considered in its de-dupe process.

Compliance checkpoints have been built so that mandatory checks such as verification with the UN sanctions list, Unlawful Activities Prevention Act (UAPA), Terrorist Financing (TF) lists is ensured during the onboarding/ underwriting stage. Also deviation has been defined wherever loans are offered to PEP customers.

## Unlawful Activities Prevention Act

- GICHFL shall not have any account in the name of individuals/ entities appearing in the lists of individuals and entities suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Councils namely the "ISIL (Da'esh) & Al-Qaida Sanctions List" and the "Taliban Sanctions List (1988 Sanctions List)" As per the terms of Section 51A of the Unlawful Activities (Prevention) Act (UAPA), 1967,.

GICHFL shall also ensure to refer to the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The aforementioned lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, shall be verified on daily basis and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by GICHFL for meticulous compliance.

- Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification.
- GICHFL shall also monitor other UNSCRs circulated by the Reserve Bank of any other jurisdictions/ entities from time to time and also monitor publicly available information for identifying countries that do not sufficiently apply FATF recommendations. The background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations shall be examined, and written findings together with all documents shall be retained and shall be made available to Reserve Bank/other relevant authorities, on request.
- GICHFL shall ensure compliance with the UAPA Order dated February 2, 2021, as per RBI Master Direction.

**Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):**

- a) GICHFL shall ensure meticulous compliance with the “Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005” laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated January 30, 2023, by the Ministry of Finance, Government of India (Annex III of the RBI Master Direction).
- b) GICHFL shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.
- c) Further, GICHFL shall run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc.
- d) In case of match in the above cases, GICHFL shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI. GICHFL shall file an STR with FIU-IND covering all transactions in the accounts, covered above, carried through or attempted.

It may be noted that, Director, FIU-India has been designated as the CNO.

- a) GICHFL may refer to the designated list, as amended from time to time, available on the portal of FIU-India.
- b) In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of Section 12A of the WMD Act, 2005, GICHFL shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post, without delay.
- c) In case an order to freeze assets under Section 12A is received by the GICHFL from the CNO, GICHFL shall, without delay, take necessary action to comply with the Order.
- d) The process of unfreezing of funds, etc., shall be observed as per paragraph 7 of the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing shall be forwarded by GICHFL along with full details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working days.

GICHFL shall verify every day, the 'UNSCR 1718 Sanctions List of Designated Individuals and Entities', as available at <https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm>, to take into account any modifications to the list in terms of additions, deletions or other changes and also ensure compliance with the 'Implementation of Security Council Resolution on Democratic People's Republic of Korea Order, 2017', as amended from time to time by the Central Government.

In addition to the above, GICHFL shall take into account – (a) other UNSCRs and (b) lists in the first schedule and the fourth schedule of UAPA, 1967 and any amendments to the same for compliance with the Government orders on implementation of Section 51A of the UAPA and Section 12A of the WMD Act.

## Money Laundering and Terrorist Financing Risk Assessment

- GICHFL shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise annually 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.
- 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, GICHFL shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with GICHFL from time to time.
- The risk assessment by GICHFL shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of GICHFL. Further, the periodicity of risk assessment exercise shall be determined by the Board of GICHFL or any Committee of the Board to which power in this regard is delegated, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.
- The outcome of the exercise 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.
- GICHFL shall apply a Risk Based Approach (RBA) and implement a CDD programme, having regard to the ML/TF risks identified and the size of business, for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard. Further, GICHFL shall monitor the implementation of the controls and enhance them if necessary.

### Introduction of New Technologies

GICHFL shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

Further, GICHFL shall ensure:

- (a) to undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and
- (b) adoption of a risk-based approach to manage and mitigate the risks through appropriate EDD measures and transaction monitoring, etc.

## Secrecy Obligations and sharing of information

- (a) GICHFL shall maintain secrecy regarding the customer information which arises out of the contractual relationship between itself and customer.
- (b) Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.
- (c) While considering the requests for data/information from Government and other agencies, GICHFL shall satisfy itself that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the transactions.
- (d) The exceptions to the said rule shall be as under:
  - I. Where disclosure is under compulsion of law
  - II. Where there is a duty to the public to disclose,
  - III. the interest of GICHFL requires disclosure and Where the disclosure is made with the express or implied consent of the customer.

## Recruitment & Training

### Recruitment

Adequate screening mechanism shall be in place as an integral part of their personnel recruitment/hiring process, including Know Your Employee / Staff policy.

### Training

A general appreciation of the background to money laundering shall be provided to all newly recruited employees, members of the sales/advisory staff who deal with customers, DSA's, administrative/operations supervisors and managers.

It will also be necessary to make arrangement for refresher training at regular intervals to ensure staff is updated with the regulatory requirements and their responsibilities under the KYC-AML guidelines. The focus of the training may 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 KYC/ AML policies and Counter Terrorist Financing guidelines of GICHFL, regulation and related issues shall be ensured.

## General

- The company will ensure that the provisions of PML Rules framed thereunder and the Foreign Contribution and Regulation Act, 1976 (wherever applicable) are strictly adhered.
- In a situation where in the KYC measures cannot be applied satisfactorily due to non-furnishing of information and/or non-cooperation by the customer, the company shall review and consult the status with its senior

management including the Principal Officer(s) and may even consider closing of the account or termination of business relationship after issuing due notice to the customer explaining the reasons for the step.

- Any changes to the list of activities or the schedule(s) can be made by the Principal Officer of the Company from time to time.
- The compliance function shall evaluate and ensure adherence to the AML & KYC policies and procedures which would be monitored/audited by the internal audit function.

## Roles and Responsibilities

Sr No.	Process	Responsibility
1.	KYC Documentation at the time of sale and verification of documents with originals	Sales & Credit
2.	Sanction loans to High-Risk Customers	Credit
3.	Screening of customers	Credit Team (at the time of onboarding) Compliance team (post onboarding)
4.	Periodic review of risk categorisation	Operations
5.	Appointment of Principal Officer (AML) & Reporting under PMLA Act and Rules	Board (for Principal Officer Appointment) & Compliance Team (reporting under PMLA)
6.	Specifically check and verify the KYC procedures and submit quarterly audit notes and compliance to the Audit Committee.	Internal Audit team
7.	Monitoring & Reporting Obligations	Compliance
8.	Information of Suspicious /attempted transactions	All employees
9.	AML Training	All employees
10.	No tipping off	All employees
11.	Maintenance of Records	
	Transaction Details	Information Technology
	Customer data, complaints, account files, business correspondence, account recovery details	Operations, Credit, Customer Service(Marketing), Collections
12.	To adhere to the requirements of the KYC policy	All employees
13.	Ensure adherence to the charter formulated towards implementation of group-wide PMLA policy	Principal Officer/Chief Compliance Officer



## Annexure I – Indicative list of customers of Risk Categorization

Individuals and entities whose identities and sources of funds are not clear and cannot be easily identified, higher due diligence is required which includes customer's background, nature and location of activity, country of origin, source of funds and his client profile, etc. besides proper identification. Company shall subject such accounts to enhanced monitoring on an ongoing basis.

### High Risk customers – Indicative list

Indicative list of High Risk customer	Description, if any
Trust/HUF/Societies/NGO/trusts, Charitable Organisation, Organizations receiving donations	Includes both registered / unregistered
Non-resident Indians / Foreign Nationals /Merchant Navy Employee	-
Politically Exposed Persons (PEPs)	<ul style="list-style-type: none"> <li>• Celebrity like actors, Business Coach etc.</li> <li>• Customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner</li> </ul>
Sleeping Partners or Partnership firms with family members acting as Sleeping Partner	Sleeping Partners refer to Partners who are partner in the form but is not actively involved in the partnership. Includes third party who acts as a sleeping partner.
Companies having close family shareholding or beneficial ownership	Close family shareholding to include non-individuals with complex layering structures under this category and Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale
Shell Companies	Companies which have no physical presence in the country in which it is incorporated. The existence simply of a local agent or low-level staff does not constitute physical presence
High net worth individuals	Any individual whose networth is >20 Crore in assets & dealers in high value or precious goods (E.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses

### Medium Risk customers – Indicative list:

Indicative list of Medium Risk customer	Description, if any
Self Employed Professional	This would include individual independent Professionals / proprietary concerns like Practicing Chartered Accountants, Practicing Company Secretaries, Lawyers, Notaries).
Self Employed Non-Professional	This category includes self-employed individuals engaged in cash intensive businesses like restaurants, retail shops, parking garages, fast food stores, travel agency, telemarketers, movie theaters, used card dealers,



	auctioneers etc. and import/ export business persons, DSA, Collection agencies and others not forming part of the list above.
Partnership firms other than firms with sleeping partners (irrespective of the business activity undertaken by them)	This includes registered partnership firms, un-registered partnership firms, Limited Liability Partnerships.
Private limited Company (irrespective of the business activity undertaken by them)	-
Association of Persons / Body of individuals (irrespective of the business activity undertaken by them)	-

### Low Risk Customers – Indicative list

For the purpose of risk categorization, individuals other than the individuals defined under the High or Medium Risk and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorized as low risk.

Indicative list would include:

- Salaried employees whose salary structures are well defined,
- People belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government departments & Government owned companies, regulators and statutory bodies, etc. In such cases, the policy may require that only the basic requirements of verifying the identity and location of the customer are to be met.

### Annexure II – List of Documents to be obtained as an identity/legal Existence and address proof

Category	Identity / Legal Existence and Address Proof Documents
Individual/Beneficial owner/ Authorised signatory or the power of attorney holder related to any legal entity	<p>ii) PAN or Form 60 (Mandatory)* and</p> <p>Copy of any of the below List of officially valid documents (OVDs) or equivalent e-document thereof:</p> <p>i) Voter ID            ii) Valid Passport            iii) Driving license            iv) Proof of possession of Aadhaar (with first eight digits masked / blacked out)            v) Job card issued by NREGA            vi) Letter issued by the National Population Register            vii) Any other document as notified by the Central Government in consultation with the Regulator.</p> <p>Note:</p>

	<p>i) Aadhaar is mandatory to be submitted for beneficiary to avail the interest subsidy under Pradhan Mantri Awas Yojana or any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016)</p> <p>ii) The KYC Identifier can be obtained with an explicit consent to download records from CKYCR</p> <p>iii) Beneficiary who do not possess the Aadhaar number or have not yet enrol for Aadhaar, shall apply for Aadhaar and provide Aadhaar enrolment ID at the time of applying for benefit. Benefits shall be given to the beneficiary subject to production of the above mentioned Officially valid document till the time Aadhaar is assigned to the beneficiary or her or his spouse.</p> <p>iv) For individual cases where current address is not updated in the above mentioned OVD submitted by client the following process to be adhered to:</p> <p>The customer needs to submit any one of the following mentioned documents as proof of address at time of login and declaration as per Annexure II with Aadhar acknowledgement for change of address (to be franked as per stamp law applicable) before disbursement.</p> <p>These cases will have to marked under PDD for submission of 'Updated OVD' for a period of three months from the date of disbursement.</p> <ol style="list-style-type: none"> <li>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)</li> <li>b. Property or Municipal tax receipt</li> <li>c. Pension or family pension payment orders (PPO's) issues to retired employees by Government Departments or Public Sector undertakings, if they contains the address</li> <li>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 license agreements with such employers allotting official accommodation</li> <li>e. Bank Passbook / Latest Bank Account Statement (First page showing complete address, in case of pass book pages showing latest transactions should also be taken on records)</li> </ol> <p>v) For the purpose of this clause, a document shall be deemed to be and OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State government or Gazette notification, indicating such change in name.</p>
<p>NRI (Non-Resident Indian)</p>	<p>PAN or Form 60 (Mandatory)* and</p> <p>Copy of any of the below List of officially valid documents: Voter ID</p>

	<p>Valid Passport  Driving license  Proof of possession of Aadhaar **  Job card issued by NREGA  Letter issued by the National Population Register  Any other document as notified by the Central Government in consultation with the Regulator.  Note 1- Where the 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.</p>
PIO (Person of Indian Origin)	<p>Copy of an any of the below 'officially valid document'.</p> <p>Voter ID  Valid Passport  Driving license  Proof of possession of Aadhaar (Refer note 1)  Job card issued by NREGA  Letter issued by the National Population Register  any other document as notified by the Central Government in consultation with the Regulator (example: PIO card issued by Govt of India)</p>
Non-Individual Entity (Proprietor)	<p>Pan Card or Form 60* of the Proprietor (Mandatory)</p> <p>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 collected:  Registration certificate including Udyam Registration Certificate (URC) issued by the Government  Certificate/ License issued by the municipal authorities under Shop and Establishment Act.  Sales and income tax returns.  (provisional/final). 23CST/VAT/ GST certificate  Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.  IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT/ License/ Certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.  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.  Utility bills such as electricity, water, and landline telephone bills. (Not older than 2 months)</p> <p>Where the Company is satisfied that it is not possible to furnish two such documents, the Company may, at their discretion, accept only one of those documents as proof of business/ activity.</p>
Non-Individual Entity (Partnership)	<p>registration certificate;  partnership deed;  Permanent Account Number of the partnership firm</p>

	<p>one copy of officially valid document and Permanent Account Numbers or Form 60 as defined in the Income-tax Rules, 1962, issued to managers, officers or employees holding an attorney to transact on the company's behalf</p> <p>Beneficial Ownership Declaration (On letter head of Company/Partnership/Trust/Body) along with the KYC documents of beneficial owners and managers, officers or employees, as the case may be, holding an attorney to transact on the firm's behalf</p> <p>The names of all the partners</p> <p>The address of registered office and the principal place of its business, if it is different All the above-mentioned documents are mandatory.</p> <p>In addition to above any of the below document needs to be submitted as an office address proof:</p> <p>Latest telephone bill (Not older than 2 months)</p> <p>Electricity bill (Not older than 2 months)</p> <p>Water bill (Not older than 2 months)</p> <p>Municipality tax receipt / property tax receipt</p>
<p>Non-Individual Entity (Company)</p>	<p>Certificate of incorporation;</p> <p>Memorandum and Articles of Association;</p> <p>Permanent Account Number of the company</p> <p>A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf;</p> <p>one copy of officially valid document and Permanent Account Numbers or Form 60 as defined in the Income-tax Rules, 1962, issued to managers, officers or employees holding an attorney to transact on the company's behalf</p> <p>Beneficial Ownership Declaration (On letter head of Company/Partnership/Trust/Body) along with the KYC documents of beneficial owners and managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf</p> <p>The names of the relevant persons holding senior management position</p> <p>The address of registered office and the principal place of its business, if it is different All the above-mentioned documents are mandatory.</p> <p>In addition to above any of the below document needs to be submitted as an office address proof:</p> <p>Latest telephone bill (Not older than 2 months)</p> <p>Electricity bill (Not older than 2 months)</p> <p>Water bill (Not older than 2 months)</p> <p>Municipality tax receipt / property tax receipt</p>
<p>Unincorporated association or a body of individuals</p>	<p>Resolution of the managing body of such association or body of individuals;</p> <p>Permanent Account Number or Form No 60 of the unincorporated association or a body of individuals</p> <p>power of attorney granted to him to transact on its behalf;</p> <p>one copy of officially valid document and Permanent Account Numbers or Form 60 as defined in the Income-tax Rules, 1962, issued to managers, officers or employees holding an attorney to transact on the company's behalf</p> <p>such information as may be required by the GICHL to collectively establish the existence of</p> <p>such association or body of individuals)</p> <p>Beneficial Ownership Declaration (On letter head of Company/Partnership/Trust/Body) along with KYC documents of its beneficial</p>

	<p>owners and managers, officers or employees, as the case may be, holding an attorney to transact on its behalf</p> <p>All the above-mentioned documents are mandatory.</p> <p>In addition to above any of the below document needs to be submitted as an office address proof:</p> <p>Latest telephone bill (Not older than 2 months)</p> <p>Electricity bill (Not older than 2 months)</p> <p>Water bill (Not older than 2 months)</p> <p>Municipality tax receipt / property tax receipt</p>
<p>Non-Individual Entity (Club / Trust / Society/ Individuals who act on behalf of above)</p>	<p>registration certificate;</p> <p>trust deed; and</p> <p>Permanent Account Number or Form No 60 of the trust</p> <p>one copy of officially valid document and Permanent Account Numbers or Form 60 as defined in the Income-tax Rules, 1962, issued to managers, officers or employees holding an attorney to transact on the company's behalf</p> <p>V) Beneficial Ownership Declaration (On letter head of Company/Partnership/Trust/Body) along with the KYC documents of beneficial owners and managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.</p> <p>The names of the beneficiaries, trustees, settlor, and authors of the trust</p> <p>The details of registered office of the trust, and</p> <p>list of trustees and KYC documents for those discharging the role as trustee and authorised to transact on behalf of the trust</p> <p>All the above-mentioned documents are mandatory.</p> <p>In addition to above any of the below document needs to be submitted as an office address proof:</p> <p>Latest telephone bill (Not older than 2 months)</p> <p>Electricity bill (Not older than 2 months)</p> <p>Water bill (Not older than 2 months)</p> <p>Municipality tax receipt / property tax receipt</p>
<p>Non-Individual Entity (HUF)</p>	<p>Copy of HUF PAN (Mandatory)</p> <p>Copy of Pan Card or Form 60 of Karta (Mandatory)</p> <p>Any of the below List of officially valid documents to be submitted for Karta:</p> <p>Voter ID</p> <p>Valid Passport</p> <p>Driving license</p> <p>Proof of possession of Aadhaar **</p> <p>Job card issued by NREGA</p> <p>Letter issued by the National Population Register</p> <p>any other document as notified by the Central Government in consultation with the Regulator</p>

**Note:**

\*Form 60 to be filled by an individual or a person (not being a company or firm) who does not have a permanent account number as specified in Rule 114B of Income Tax rule, 1962. Click on below link to download Form 60 - <http://www.incometaxindia.gov.in/forms/income-tax%20rules/10312000000007944.pdf>

\*\*Wherever Aadhaar number is provided by client as officially valid document (OVD), reporting entity (GICHFL) shall redact or black out the Aadhaar Number through appropriate means.

**Application Form with Photograph**

Description	Type of Documents
Application Form	Duly completed application form signed by all the applicants/ co-applicants/ guarantors. Applicants should also sign across the photograph and application form. Latest passport size colour photographs of all applicant / co-applicants / guarantors with cross sign. Any corrections / overwriting on the application form should be countersigned by the respective applicant / co applicant / guarantor.

**Signature Verification**

Description	Type of Documents
Signature Verification (Individual)	Copy of Pan Card Copy of Laminated Driving License (permanent only) Copy of Passport Bank Verification (Only Scheduled Commercial Banks) Government ID card for Govt. Employees Copy of entire Registered sale deed showing photo and signature Login/Processing Fee Cheque Clearance ECS Mandate certified by authorised official of the Bank from where repayment is to be made (Note - There could be instances wherein applicant /co-applicant/ guarantor do not have any signature verification proof as above, in such cases a declaration should be obtained.(duly executed on stamp paper).
Signature Verification (Authorized Signatory)	Copy of Pan Card Copy of Passport Banker's verification of the entity's Authorized Signatory from where ECS is issued.



All documents provided by the customer (for applicant/co-applicant /guarantor) should be sighted in original and verified by the GICHFL Employee and signed and stamp with “Original Seen and Verified” with date, employee ID and Employee Name.

## Abbreviations

GICHFL / the Company	GIC Housing Finance Limited
AML	Anti-Money Laundering
BO	Beneficial Owner
CDD	Customer Due Diligence
CERSAI	Central Registry of Securitization Asset Reconstruction and Security Interest of India
CIP	Customer Identification Procedure
CKYC	Central KYC Registry
CNO	Chief Nodal Officer
CTR	Cash Transaction Report
EDD	Enhanced Due Diligence
FIU-IND	Financial Intelligence Unit – India
FATF	Financial Action Task Force
HFC	Housing Finance Company
KYC	Know Your Customer
KYC-AML Policy	Know Your Customer and Anti Money Laundering Policy
ML	Money Laundering
NHB	National Housing Bank
OVD	Officially Valid Document
PEP	Politically Exposed Person
PMLA	Prevention of Money Laundering Act
RBI	Reserve Bank of India
STR	Suspicious Transaction Report
TF	Terrorist Financing
UAPA	Unlawful Activities Prevention Act
UNSCR	United Nations Security Council Resolution
V-CIP	Video based Customer Identification Procedure
WMD Act	Weapons Mass Destructive Act