GANPATI FINLEASE PRIVATE LIMITED

KNOW YOUR CUSTOMER AND ANTI-MONEY LAUNDERING POLICY

Version Control Version	**Adoption/** **Amendment Date by Board**	**Prepared / Changed by**	**Last Review Date**
1	1 Apr 2025	Legal & Compliance	N.A.

KNOW YOUR CUSTOMER & ANTI-MONEY LAUNDERING POLICY

("KYC & AML POLICY")

- **Background**

Ganpati Finlease Private Limited (hereafter referred to the "**Company**") is a private limited company incorporated under the provisions of the Companies Act, 2013 and is a non-banking finance company ("**NBFC**") registered with Reserve Bank of India ("**RBI**").

In terms of the provisions of Prevention of Money Laundering Act, 2002 and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, as amended from time to time, RBI has issued comprehensive 'Know Your Customer' ("**KYC**") directions applicable to all NBFCs, as amended from time to time. In view of the same, the board of directors of the Company has duly approved and adopted this policy framework on anti-money laundering ("**AML**"), countering financing of terrorism ("**CFT**") and KYC measures in line with RBI directions.

The Company has formulated this KYC & AML Policy based on RBI's Master Direction- Know Your Customer (KYC) Direction, 2016, dated 25th February 2016, updated from time to time ("**MD**"), the provisions of Prevention of Money Laundering Act, 2002 and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 and it is to be read in conjunction with and shall stand auto-corrected with related operational guidelines issued or any changes/modifications which may be advised from time to time by the RBI and/or other regulators.

1. Objectives

1.
2. **1.1.** To prevent money laundering or terrorist financing activities; **"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.
3. **1.2.** To enable the Company to know and understand its customers and their financial dealings better, which in turn help the Company to manage its risks prudently.
4. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.
5. To comply with applicable laws and regulatory guidelines.
6. To ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures.
7.

2. Definitions

1.
2. Terms used in this KYC & AML Policy shall, unless contrary to the meaning thereof, have the meaning as assigned to them in the MD, Prevention of Money Laundering Act, 2002 and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, Aadhaar and Other Laws (Amendment) Act, 2019 and the rules and regulations made thereunder, as amended from time to time.

1. **2.1. "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.
3. **2.2. "Periodic Updation"** means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank.

1. **2.3. "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.

1. **2.4. "Customer Due Diligence (CDD)"** means identifying and verifying the Customer and the beneficial owner using reliable and independent sources of identification.

2.

Explanation – The CDD, at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include:

a. (a) Identification of the Customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable.

b.

c. (b) Taking reasonable steps to understand the nature of the Customer's business, and its ownership and control;
"Designated Director" means the Chief Executive Officer, duly authorized by the Board of Directors of the Company to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules.

1.

2. (c) Determining whether a customer is acting on behalf of a beneficial owner and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.

1. **2.5. "Designated Director"** means the Chief Executive Officer, duly authorized by the Board of Directors of the Company to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules.

2.

3. **2.6. "Equivalent e-document"** means an electronic equivalent document, issued by the issuing authority 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.

4.

5. **2.7. "Officially Valid Document" ("OVD")** means the passport, the driving license, 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,

6.

a. 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.

a. 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 and leave and licence agreements with such employers allotting official accommodation.

a. C. the Customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above.

a. 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.

3. KYC Process

3.1. Customer Acceptance Policy ("**CAP**") as set down under **Annexure 1**. Customer Acceptance Policy will treat all clients at par without even discriminating against members of the general public and will not result in denial of financial facility to members of the general public, especially those, who are financially or socially disadvantaged.

3.2. Customer Identification Procedures ("**CIP**") as set down under **Annexure 2**.

3.3. Customer Due Diligence Procedures: The features to be verified and documentary proof required from Customers and/or their Power of Attorney (POA) holder, and/ or authorised signatory as set down under **Annexure 3**.

1. Risk Management - The Company will have a risk-based approach for categorisation which includes the following:

    1. Customers will be categorized as low, medium and high-risk category, based on the assessment and risk perception of the Company.
    2. Risk categorization will be undertaken on the basis of parameters such as Customer's identity, social/financial status, nature of business activity, and information about the clients' business and their location, geographical risk covering Customers as well as transactions, type of products/ services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc mode of sourcing, nature of underlying loan 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.
    3. The risk categorization of a Customer and the specific reasons for such categorization will be kept confidential and will not be revealed to the Customer to avoid tipping off the Customer.

However, while preparing Customer profile, the Company will take care to seek only such information from the Customer which is relevant to the risk category and is not intrusive. FATF Public Statement, the reports and guidance notes on know your Customer/anti money laundering issued by the Indian Banks Association and other agencies, etc. may also be used by the Company in risk assessment.

1. Monitoring of transactions- The Company can effectively control and reduce the risk only if it has an understanding of the normal and reasonable activity of its Customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. The Company shall put in place an appropriate system / mechanism to throw alerts when the transactions are inconsistent with risk categorization as set out in paragraph 3.4 above and the updated profile of Customers. The Company should ensure that a record of transactions with Customers is preserved and maintained as per the requirements set out in paragraph 6 and 7 below.

1. **Responsibility**

4.1. The Company has a Designated Director nominated, appointed, duly authorised and designated by its Board of Directors for the purpose of ensuring overall compliance by the Company with the obligations imposed under Act and its Rules. The Company has communicated the name, designation, address and contact details of the Designated Director to the FIU-IND and RBI. The Designated Director of the Company is a person other than Principal Officer of the Company.

1. **4.2.** The Company has also appointed the 'Principal Officer', who is an officer at the management level nominated by the board of directors of the Company and who is responsible for ensuring compliance with RBI

requirements and such other requirements, monitoring transactions and sharing and reporting information as required under applicable law and regulations. The Company has communicated the name, designation, address and contact details of the Principal Officer to the FIU-IND and RBI.

2.
3. **4.3.** The Company will ensure compliance with its KYC & AML Policy through:

1. The C-Suite Executives and the Departmental Heads (*for each of Sales, Credit, Collections, Operations, Digital, Human Resources & Administration functions*) will constitute senior management of the Company ("**Senior Management**") for the purpose of KYC compliance and for its effective implementation.
2. Allocation of responsibility for effective implementation of policies and procedures.
3. Concurrent/ internal audit system to verify the compliance with KYC/AML policies and procedures.
4. Submission of quarterly audit reports of the auditors and compliance to its Board.
5. The Senior Management of the Company will play an important role in providing an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements. The Company will ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

1. **4.4.** The Company will ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

5. On-going due diligence ("ODD") & evaluation

5.1. The Company will carry out on-going due diligence of Customers with respect to the business relationship with every Customer and closely examine the transactions in order to ensure that they are consistent with their knowledge of the Customer, business and risk profile and, the source of funds/wealth. The Company can effectively control and reduce the risk only if it has an understanding of the normal and reasonable activity of the Customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the overarching principle for ODD is that the extent of ODD/monitoring will be aligned with the risk category of the Customer. High-risk Customers will be subjected to intensified monitoring in accordance with MD.

1. The Company has adopted 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. Full KYC exercise will be carried out, at least once in every two years for high-risk Customers, at least once in every eight years for medium risk Customers and at least once in every ten years for low-risk Customers, from the date of opening of account/last KYC updation. Individual Customers:

A. Individual Customers:

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

a. b) Change in address: In case of a change only in the address details of the Customer, a self-declaration of the new address will 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 /mobile application of the Company), letter etc., and the declared address will be verified by the Company through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables. etc. Further, the Company, at their option, may obtain a copy of OVD or deemed OVD or Equivalent e-documents thereof, for the purpose of proof of address, declared by the Customer at the time of Periodic Updation.

a. C) Accounts of Customers, who were minor at the time of opening account, on their becoming major: In case of Customers for whom account was opened when they were minor, fresh photographs shall be obtained on their becoming a major and at that time it shall be ensured that CDD documents as per the current CDD standards are available with the Company. Wherever required, the Company may carry out fresh KYC of such customers i.e., customers for whom account was opened when they were minor, on their becoming a major.

1. d) Aadhaar OTP based e-KYC in non-face to face mode may be used for Periodic Updation. Declaration of current address, if the current address is different from the address in Aadhaar, will not require positive confirmation in this case. The Company will ensure that the mobile number for Aadhaar authentication is same as the one available with them in the Customer's profile, in order to prevent any fraud.
2.
3. **B. Customers other than individuals:**
4.

a. No change in KYC information: In case of no change in the KYC information of the legal entity customer ("**LE customer**"), a self-declaration in this regard shall be obtained from the LE customer through its email id registered with the Company, ATMs, digital channels (such as online banking / internet banking, mobile application of the Company), letter from an official authorized by the LE customer in this regard, board resolution, etc. Further, the 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, the Company shall undertake the KYC process equivalent to that applicable for on boarding a new LE customer.

C. Additional measures: In addition to the above, Company shall ensure that:

1.
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 Company has expired at the time of Periodic Updation of KYC, the Company shall undertake the KYC process equivalent to that applicable for onboarding 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. 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 make available the facility of Periodic Updation of KYC at any branch. The Company has adopted a risk-based approach with respect to periodic updation of KYC.

4. The Company will advise the Customers that in order to comply with the Rules, in case of any update in the documents submitted by the Customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary, Customers will submit to the Company the update of such documents. This will be done within 30 days of the update to the documents for the purpose of updating the records at the Company' end.

5. In case of existing Customers, the Company will obtain the Permanent Account Number or Equivalent e-document thereof or Form No.60 of the Customer failing which the Company will temporarily cease operations in the account till the time the Permanent Account Number or Equivalent e-document thereof or Form No. 60 is submitted by the Customer. Provided that before temporarily ceasing operations for an account, the Company will give the Customer an accessible notice and a reasonable opportunity to be heard. Further, the Company will provide appropriate relaxation(s) for continued operation of accounts for Customers who are unable to provide Permanent Account Number or Equivalent e-document thereof or Form No. 60 owing to injury, illness or infirmity on account of old age or otherwise, and such like causes. Such accounts will, however, be subject to enhanced monitoring. Provided further that if a Customer having an existing account-based relationship with the Company gives in writing to the Company that he does not want to submit his Permanent Account Number or Equivalent e-document thereof or Form No.60, the Company will close the account and all obligations due in relation to the account will be appropriately settled after establishing the identity of the Customer by obtaining the identification documents as applicable to the Customer.

1. A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures has been put in place. High risk accounts

will be subjected to intensify monitoring.

2. As a risk-mitigating measure for such accounts, the Company will ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the Customer registered with Aadhaar. In case of request of change of mobile number from the Customer, below steps to be followed:

1. The Customer to initiate formal request from registered email id or letter to the Company for change of mobile number, (the mobile number should be linked with Aadhaar),
2. On receipt of formal request from the Customer, the Company will initiate Aadhaar based OTP verification of mobile number,
3. Post successful verification of mobile number, the Customers' details to be updated in the records of the Company.

1. For ongoing due diligence, the Company may consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) technologies to support effective monitoring.

6. Record Management

6.1. All transaction records between the Company and the Customer, both domestic and international, including KYC documents obtained from Customers will be maintained by the Company for a period of Five (5) years from the date of transaction.

6.2. The Company will preserve the records pertaining to the identification of the Customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;

6.3. The Company will make available swiftly the identification records and transaction data to the competent authorities upon request;

1. The Company will maintain proper records of the identity and address of their Customer, and proper records, including in respect of transactions prescribed under rule 3 of Rules.

1. The Company will maintain all necessary information in respect of transactions prescribed under rule 3 of Rules, so as to permit the reconstruction of the individual transaction including the following information:

b. Nature of the transactions,
c. Amount of the transaction and the currency in which it was denominated,
d. The date on which the transaction was conducted,
e. Parties to the transaction

1. The Company has 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.
2. The Company will maintain records of the identity and address of their Customer, and records in respect of transactions referred to in rule 3 of Rules in hard or soft format.

Explanation. – For the purpose of this Clause, the expressions "records pertaining to the identification", "identification records", etc., will include updated records of the identification data, account files, business correspondence and results of any analysis undertaken.

1. The Company shall ensure that in case of Customers who are non-profit organisations, the details of such Customers are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, the Company shall register the details on the DARPAN Portal. The Company shall also maintain such registration records for a period of five years after the business relationship between the Customer and the Company has ended or the account has been closed, whichever is later.

1. **Monitoring of Transactions**

1. On-going monitoring is an essential element of effective KYC procedures. Monitoring of transactions and its extent will be conducted taking into consideration the risk profile and risk sensitivity of the account.
2. The Company will pay special/ close attention to, and monitor all large, complex, unusually large transactions, all unusual patterns, inconsistent with the normal and expected activity of the Customer, which have no apparent economic rationale or visible lawful purpose. High risk Customers have to be subjected to intensified monitoring.

1. **Reporting Transactions**
    1. The Company will, to the extent applicable to it, ensure compliance with the reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS). The Company will adhere to provisions of Income Tax Rules.
    2. The Company shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of rule 7 thereof.
    3. The Company will not put any restriction on operations in the accounts where a suspicious transaction report ("STR") has been made. Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the Customers are put in to use as a part of effective identification and reporting of suspicious transactions It should also be ensured that there is no tipping off to the Customer at any level.

9. Internal ML/ TF Risk Assessment

The Company will 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.

The assessment process considers 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 will take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share from time to time. Further, the risk assessment by the Company will be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company.

Also, the Company will apply a Risk Based Approach (RBA) for mitigation and management of the risks (identified on their own or through national risk assessment) and has board approved policies, controls and procedures in this regard. The Company will implement the Customer Due Diligence programme, having regard to the ML/TF risks identified and the size of business. Further, the Company will monitor the implementation of the controls and enhance them if necessary.

The periodicity of such risk assessment exercise will be determined by the Board, in alignment with the outcome of the risk assessment exercise. However, it will be reviewed at least annually.

The outcome of the exercise will be put up to the Board and should be available to competent authorities and self-regulating bodies.

10. Know-Your-Employee & Employee Training

The Company has implemented an employee due diligence program or a Know-Your-Employee process ("**KYE**") that protects against money laundering and terrorist financing, to ensure that the risk from internal functions such as its employees are mitigated, and the employee is suitable for the tasks assigned, and to protect against reputational, legal, and operational risks and help identify red flags.

The KYE covers the entire employment lifecycle with the employee (i.e., from the recruitment process, ongoing employee relationship and if need be, termination of employment). The KYE approach is risk-based, and more stringent screening procedures are required for employees that function in high-risk roles. When an employee is moving to a new role, the Company shall determine (based on the risk assessments and controls) whether the new role requires the employee to update or undertake a rescreening process and the frequency, and if their role puts them in a position to facilitate the commission of a ML/TF offence. These procedures must be documented and include disciplinary actions if it is detected that that information provided by an employee is false.

- A. To screen prospective employees, the Company shall ask them to provide the following information to assist with determining their suitability:
-
- - Employment history
- - Reference checks – character and from previous employers
- - Identify and verify identity
- - Police verification and background check, as required based on risk assessment
- - For positions that require technical qualifications and/or practicing certificates, such as a lawyer or an accountant, a confirmation that the person is a member of the relevant professional association
- - Academic qualifications (checking the authenticity of academic qualifications depending on risk of role and knowledge of the prospective employee)
- - Credit check

The Company will keep up-to-date records of employee identification information, certifications, employment history, performance reviews, and so on to know if an employee's financial risk level changes. The Company shall also carry out checks to ensure that the employee is not subject to any court or legal action and if the employee has lived in high-risk countries or abroad for an extended period that may require further checks.

- B. The Company has also put in place a code of conduct or employee handbook or ethics that outlines the Company's employment conditions including conflict of interest, confidentiality policies and sanctions that the employees must abide by. Moreover, human resources policies and processes related to termination of engagement that protect sensitive information and ensure confidentiality of information is maintained beyond employment are also maintained by the Company and the employees are required to abide by them.

1. C. Safeguards should be implemented by the Company to avoid employees abusing their positions. For instance, the Company should only give an employee access to such information and systems that is related to his/her roles and responsibilities. In addition, it should monitor the employees and conduct regular audits of their activity. Managers should maintain frequent communication with the employees under their supervision. They should discuss employee responsibilities, work environment/culture, role and/or career goals, and work-life balance.
2.

In addition to the above, to make the KYE programme more efficient, an on-going employee training programme will be put in place so that the employees are adequately trained in the KYC/AML/CFT policy. The focus of the training will be different for frontline staff, compliance staff and staff dealing with new Customers. The front desk staff will 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 the KYC/AML/CFT policies of the Company, regulation and related issues will be

ensured will be put in place in AML procedures. The Company will prepare specific literature/pamphlets etc.to educate the Customer of the objectives of the KYC programme.

The Company should also inform the employees of what to expect – and what's expected of them – to keep the business secure. The Company's employees should be aware of penalties and sanctions that apply in case of confidentiality breaches or bad behaviour. Periodic training programmes will be organized for employees to have adequate screening mechanism, as an integral part of their personnel recruitment/hiring process.

1.
2. The Company will ensure that the staff dealing with/ being deployed for KYC/AML/CFT matters have high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally. The Company will also strive to develop an environment which fosters open communication and high integrity amongst the staff.

11. Confidentiality

The Company will maintain secrecy regarding the Customer information which arises out of the contractual relationship between the Company and Customer.

Information collected from Customers for the purpose of opening of account will be treated as confidential and details thereof will not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the Customer. The exceptions to the said rule will be as under:

1. **11.1.** Where disclosure is under compulsion of law;
2. **11.2.** Where there is a duty to the public to disclose;
3. **11.3.** The interest of the Company requires disclosure and;
4. **11.4.** Where the disclosure is made with the express or implied consent of the Customer.

12. Other Information 11

1. **12.1.** The Company will pay adequate attention to any money-laundering and financing of terrorism threats that may arise from new or developing technologies and it will be ensured that products/services/technologies.
2.
3. **12.2.** Unique Customer Identification Code ("UCIC") will be allotted while entering new relationships with the individual Customers as also the existing individual Customers by the Company.
4.
5. **12.3.** The Board of the Company will review the KYC & AML Policy on an annual basis or at earlier intervals, if there any regulatory changes necessitating such interim reviews.

13. Introduction of New Technologies:

1.
2. **13.1.** The Company will 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.

13.2. Further, the Company will ensure:

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

14. Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967:

The Company will ensure that in terms of the Unlawful Activities (Prevention) Act, 1967 and amendments thereto (UAPA), the name of the Customer does not appear in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council. The Company will also 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, will be verified on daily basis and any modifications to the lists in terms of additions, deletions or other changes will be taken into account by the Company for meticulous compliance.

Freezing of Assets under Section 51A of UAPA, 1967: The procedure laid down in the UAPA Order dated February 2, 2021, will be strictly followed by the Company and meticulous compliance with the Order issued by the Government will be ensured.

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

The Company will 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 September 1, 2023, by the Ministry of Finance, Government of

India. The Company will 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. Additionally, the Company will also 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.

16. Combating Financing of Terrorism

The Company will consider the Financial Action Task Force ("**FATF**") Statements circulated by the Reserve Bank of India from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations. The Company will apply enhanced due diligence measures, which are effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF. Special attention will be given to business relationships and transactions with individuals (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

17. Reporting to Financial Intelligence Unit – India

Information / reporting of records, including with respect to cash transactions and suspicious transactions, as required in terms of the Act and the Rules made thereunder will be furnished to the Director, FIU-IND, in the prescribed formats and within prescribed time frame under the Act and the Rules made thereunder.

The Company, its directors, officers, and all employees will ensure that the fact of maintenance of records referred to in rule 3 of Rules and furnishing of the information to the Director, FIU-IND is confidential. However, such confidentiality requirement will not inhibit sharing of information under paragraph 4(b) of MD of any analysis of transactions and activities which appear unusual, if any such analysis has been done.

18. Review / Revision of the Policy

The Board shall review the Policy annually or earlier if considered necessary and undertake all steps in that regard. This Policy should always be read in conjunction with RBI guidelines, directives and instructions, from time to time.

-
-

ANNEXURE 1

CUSTOMER ACCEPTANCE POLICY

In addition to the provisions of the Company's Customer Acceptance Policy, the Company will ensure that:

- a. No account will be opened by the Company in anonymous or fictitious/benami names.
- b. No account will be opened where the Company is unable to apply appropriate CDD measures, either due to non-cooperation of the Customer or non-reliability of the documents/information furnished by the Customer. The Company will consider filing a STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to 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 will be as specified in **Annexure 3** of this KYC &AML Policy and as amended or specified from time to time. Any exceptions will be discussed with the Principal Officer and the decision of Principal Officer (in compliance with the KYC & AML Policy) will be final and binding.
- e. If any additional information, is required to be obtained from the Customer(s), which is not specified in this KYC & AML Policy, the Company will obtain such additional information with the explicit consent of the Customer.
- f. The Company will apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant Customer of the Company desires to open another account with the Company, there will be no need for a fresh CDD exercise.
- g. CDD procedure is followed for all the joint account holders, while opening a joint account.
- h. Circumstances in which, a Customer is permitted to act on behalf of another person/entity, is clearly spelt out.
- i. Suitable system is 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 indicated in Chapter IX of the MD.
- j. Details of accounts resembling any of the individuals/entities in the lists will be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated February 21, 2021.
- k. The Company will take into account other UNSCRs and lists in the first and 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.
- l. Where Permanent Account Number (PAN) is obtained, the same will be verified from the verification facility of the issuing authority. Where Goods and Services Tax (GST) details are available, the GST number will be verified from the search/verification facility of the issuing authority.
- m. Where the Company forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the Customer, it will not pursue the CDD process, and instead file an STR with FIU-IND.
- n. Where an Equivalent e-document is obtained from the Customer, the Company will verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).
- o. Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.

p. Customer Acceptance Policy shall not result in denial of banking/financial facility to members of the general public, especially those, who are financially or socially disadvantaged.

ANNEXURE 2

CUSTOMER IDENTIFICATION PROCEDURES

Customer identification means identifying the Customer and verifying his / her / its identity by using reliable, independent source documents, data or information while establishing a relationship. The Company will obtain sufficient information such as PAN, Voter ID card / Passport / Officially Valid Documents, etc. necessary to establish, to its satisfaction, the identity of each new Customer, whether regular or occasional and the purpose of the intended nature of relationship.

The Company will undertake identification of Customers in the following cases:

- a. Commencement of an account-based relationship with the Customer.
- b. When there is a doubt about the authenticity or adequacy of the Customer identification data it has obtained.
- c. 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.
- d. 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.

e. As and when applicable, selling third party products as agents, selling their own products and any other product for more than rupees fifty thousand

ANNEXURE 3

MANDATORY INFORMATION TO BE SOUGHT FOR KYC AND PERIODIC UPDATION

a.
b. 1.1 Certified documents or its Equivalent e-documents, as set out under the MD, will be obtained from the individual at the time of establishing an account-based relationship.
c.
d. 1.2 The Customer Due Diligence/ verification of the Company's individual Customers may be carried out by the Company itself or through an independent agency/ third party. For the purpose of verifying the identity of Customers at the time of commencement of an account-based relationship, the Company, may rely on Customer Due Diligence done by a third party, subject to the following conditions:

a. 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.

a. b) Adequate steps are taken by the Company to satisfy themselves that copies of identification data and other relevant documentation relating to the Customer Due Diligence requirements will be made available from the third party upon request without delay.

a. 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 Act.

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

a. e) The ultimate responsibility for Customer Due Diligence and undertaking enhanced due diligence measures, as applicable, will be with the Company.

a. f) Decision-making functions of determining compliance with KYC norms are not outsourced.

a. g) While undertaking identification of Customers, introduction is not sought while opening accounts.