POLICY ON KNOW YOUR CUSTOMER (KYC) & ANTI MONEY LAUNDERING (AML)

Version Number	Prepared by	Version Control department	Approval Date	Version Details
1.	Yash Panchal	Company Secretary and Legal	29.06.2019	Initial Policy
2	Yash Panchal	Company Secretary and Legal	04.06.2021	Amendment
3	Yash Panchal	Company Secretary and Legal	03.06.2022	Amendment
4	Yash Panchal	Company Secretary and Legal	23.05.2023	Amendment
5	Yash Panchal	Company Secretary and Legal	15.12.2023	Amendment
6	Yash Panchal	Company Secretary and Legal	02.12.2024	Amendment

Content of the Policy

KNOW YOUR CUSTOMER (KYC) & ANTI MONEY LAUNDERING (AML) POLICY (VERSION 5)

1 INTRODUCTION.

In order to prevent banks and other financial institutions from being used as a channel for Money Laundering (ML)/ Terrorist Financing (TF) and to ensure the integrity and stability of the financial system, efforts are continuously being made both internationally and nationally, by way of prescribing various rules and regulations are prescribed nationally and internationally. Internationally, the Financial Action Task Force (FATF) which is an inter-governmental body established in 1989 by the Ministers of its member jurisdictions, sets standards and promotes effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. India, being a member of FATF, is committed to upholding measures to protect the integrity of the international financial system.

The Prevention of Money Laundering Act, 2002 (PML) and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, form the legal framework on Anti-Money Laundering (AML) and Countering Financing of Terrorism (CFT). is enacted to prevent and control money laundering and to confiscate and seize the property obtained from the laundered money.

In terms of the provisions of the PML Act, 2002 and the PML Rules, 2005, as amended from time to time by the Government of India, Regulated Entities (REs) are required to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transaction.

Accordingly, in compliance with the PML Act and PML Rule and RBI Master Know Your Customer (KYC) Direction, 2016 issued by the the Government of India and RBI (as amended from time to time), This policy applies to all categories of Lending products and services offered by the Company.

2 OBJECTIVE & APPLICABILITY.

The primary objective is to prevent the Company from being used, intentionally or unintentionally by criminal elements for money laundering activities. The guidelines mandate the Company to determine the true identity, ownership of accounts, source of funds, the nature of the customer's business, and the reasonableness of operations in the account in relation to the customer's business, etc. which in turn helps the Company to manage its risks prudently.

Accordingly, The Board of Directors, Management and all employees shall adhere to these standards to protect the Company and its reputation from being misused for money laundering and/or terrorist financing or other illegal purposes.

All departments shall ensure that appropriate KYC procedures issued from time to time are duly applied before introducing new products/services/technologies.

3 DEFINITION.

i. Aadhaar number shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016);

ii. 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;

iii. Beneficial Owner (BO) shall mean where

a) the customer is a company the beneficial owner is 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.

b) where the customer is a partnership firm, the beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more juridical person, has ownership of entitlement to more than 10%. of capital or profits of the partnership or who has the right to control the management or policy decision;

c) where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than 15% (fifteen) per cent. of the property or capital or profits of such association or body of individuals;

where no natural person is identified under (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;

d) where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10% 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; and

e) where the customer or the owner of the controlling interest is an entity listed on a stock exchange in India, or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions notified by the Central Government, or it is a subsidiary of such listed entities, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.

Controlling ownership interest means ownership of or entitlement to more than 10% of shares or capital or profits of the company;

Control shall include the right to appoint the 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;

iv. Customer means a person who is engaged in a financial transaction or activity with a Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

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

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) Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;
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.

vi. Obtaining a certified copy shall mean comparing the copy of the proof of possession of the Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorized officer of the Company.

vii. Designated Director means the Managing Director or a whole-time Director, duly authorized by the Board of Directors to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules.

viii. Digital KYC means the capturing live photo of the customer and an 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 authorized officer of the Company.

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

x. 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.

xi. Know Your Client (KYC) Identifier means the unique number or code assigned to a customer by the Central KYC Records Registry.

xii. Non-face-to-face customers mean customers who open accounts without visiting the branch/offices of the REs or meeting the officials of REs.

xiii. 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. In case the address is not updated on the OVD, 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; (ii) property or Municipal tax receipt; (iii) pension or family pension payment orders subject to submission OVD with current address within a period of three months.

xiv. offline verification means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by regulations.

xv. On-going Due Diligence means regular monitoring of transactions in accounts to ensure that those are consistent with RE's knowledge about the customers, customers' business and risk profile, the source of funds/wealth.

xvi. Person has the same meaning assigned in the Act and includes:
a) an individual,
b) a Hindu undivided family,

c) a company,
d) a firm,
e) an association of persons or a body of individuals, whether incorporated or not,

every artificial juridical person, not falling within any one of the above person and any agency, office, or branch owned or controlled by any of the above persons (a to f).

xvii. 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 and important political party officials.

xviii. Principal Officer means an officer at the management level nominated by the RE, responsible for furnishing information as per rule 8 of the Rules

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

a) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
b) appears to be made in circumstances of unusual or unjustified complexity; or
c) appears to not have an economic rationale or bona-fide purpose; or
d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

xx. Video based Customer Identification Process (V-CIP) mean an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the Company 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 an audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face CIP for the purpose of this Master Direction.

All other expressions, unless defined herein, shall have the same meaning as have been assigned to them in the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 and RBI's Master Direction - Know Your Customer (KYC) Direction, 2016 as amended from time to time.

4 MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT.

The Company will carry out Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment exercise as and when required (at least annually) to identify, assess, and take effective measures to mitigate the money laundering and terrorist financing risk arising from the customer, clients, countries or geographic areas, products, services, transactions or delivery channels, etc.

The risk assessment should be commensurate to size, geographical presence, complexity of activities/structure, etc. of the Company. The risk assessment approach take cognizance of the overall sector-specific vulnerabilities, if any, which the regulator may share from time to time.

The Company should place the outcome of the assessment before the Board. The Company should apply Risk Based Approach (RBA) for mitigation and management of identified risks and shall monitor the implementation of the controls and if required enhance the controls.

5 KEY ELEMENTS OF THE POLICY.

The Company is hereunder framing the KYC policy incorporating the following four key elements:

a) Customer Acceptance Policy ("CAP");
b) Customer Identification Procedures ("CIP");
c) Customer Due Diligence (CDD);
d) Risk Management; and
e) Monitoring of Transactions

6 CUSTOMER ACCEPTANCE POLICY (CAP).

The company shall follow the following norms while accepting, dealing and taking the decision to grant credit facility to customers.

The Company will ensure that it will:

a) not open an account in an anonymous/fictitious/benami name or where the Company is unable to do customer due diligence (CDD) on account of non-cooperation of the customer or non-reliability of the documents/ information furnished by the customer.
b) not sanction any credit facility to minors nor minor will be part of the credit guarantee.
c) carry out full-scale customer due diligence (CDD) for all customers before granting credit facilities and financial products/services.
d) obtain mandatory KYC documents as specified in the policy and other information while onboarding and during the periodic updation of the account.
e) obtained explicit consent, if required for taking optional/additional information from the customers as per the Company risk assessment and KYC guidelines issued by the Government of India or the RBI from time to time.
f) undertake the CDD procedure for all new applicants and guarantors at the Unique Customer Identification Code (UCIC) level. Fresh CDD procedure is not required for an existing KYC compliant customer.
g) match the identity of the customer with the negative list of persons or entities issued by the RBI and FUIIND from time to time.
h) may permit any other person/entity to act on behalf of the customer as per circumstances, if any.
i) verify the PAN from the NSDL or any other authority which is authorised to issue PAN and verify the digital signature where the customer has provided an equivalent e-document to the Company.
j) verify the GST number and GST details from the GST portal using the search/verification facility.

k) file suspicious Transaction Reporting (STR), if necessary, with FIUIND, where the customer identity is unknown and CDD procedures is not complied with due to customer cooperation or non-reliability of documentation produced to the Company.

l) Photocopies of documents submitted by the customer shall be compulsorily verified with original, with signature/confirmation of the person verifying it shall be put as proof verification.

7 CUSTOMER IDENTIFICATION PROCEDURE (CIP).

Customer identification means identifying the customer and verifying their identity by using reliable and independent sources of documents, data or information to ensure that the customer to be onboarded is not a fictitious person.

The Company will undertake CIP:

a) before onboarding the customer.

b) when there is a doubt about the authenticity or adequacy of identification data already obtained.

c) while selling own and third-party products as agent and any other product for more than Rs. 50,000 and where the customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50,000.

The Company may rely on the due diligence done by the third party subject to the following conditions that;

a) Records and Information are immediately transferred to the Company from the third party or CKYC.

b) 3rd party are located within the boundaries of India and 3rd party is regulated, supervised or monitored, and the third party is in compliance with requirements and obligations mentioned under the PML Act.

c) Copies of data, documents, and information will be made available upon request without delay.

d) 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.

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

8 CUSTOMER DUE DILIGENCE PROCEDURES (CDD).

The company shall obtain the following documents or equivalent e-documents from the customer for conducting identification and due diligence. As part of the Loan documents, the company takes consent under the loan documentation to retrieve, verify and report the KYC information with the regulators.

8.1 The List of Documents to be collected and CDD measure performed for different type of customer are as follow;

Sr. No	Type	Type of Documents or the equivalent e-documents to be collected from the customer
1.	Individual, Beneficial Owner, Authorised signatory and the power of Attorney Holder. Identification and address proof	Any two of the following documents (PAN is mandatory). ➢ PAN Card/Form 60 ➢ Aadhaar Card ➢ Passport ➢ Voter's Identity Card issued by Election Commission ➢ Driving License ➢ job card issued by NREGA duly signed by an officer of the State Government and a Letter issued by the National Population Register containing details of name and address. Where the above-mentioned documents do not have updated address, the Company shall take for the limited purpose of proof of address: ➢ utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); ➢ property or Municipal tax receipt; ➢ pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; ➢ 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.
2.	Sole Proprietary firms	In addition to the documents mentioned in point no. 1, any two of the following documents as Proof of business/ activity: ➢ Registration certificate including Udyam Registration Certificate (URC) issued by the Government. ➢ Certificate/license issued by the municipal authorities under the Shop and Establishment Act. ➢ Sales and income tax returns. ➢ CST/VAT/ GST certificate (provisional/final). ➢ Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.

Sr. No	Type	Type of Documents or the equivalent e-documents to be collected from the customer
		➢ IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or 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 acknowledgment) 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, landline telephone bills, etc. The Company may, at their discretion, accept only one of those documents as proof of business/activity and such other documents in respect of the nature of business and financial status of an entity.
3.	Partnership Firm	In addition to the documents mentioned in point no. 1, relating to beneficial owners, managers, officers, or employees or authorized signatories or holders of PoA to transact on its behalf. **Certified copy of all the below documents**; ➢ Registration certificate ➢ Partnership deed, if any ➢ PAN Card/Form 60. ➢ Name of all partners ➢ Proof of address of the Registered office and Principal Place of business, if both are different. ➢ Business activity proof (as mentioned in point no. 2) ➢ Such other documents in respect of the nature of business and financial status of an entity.
4.	Legal Entity	In addition to the documents mentioned in point no. 1, relating to beneficial owner, managers, officers or employees, or authorized signatories or holders of PoA to transact on its behalf. **Certified copy (by Director/CS/CFO) of all the below documents;** ➢ Certificate of incorporation ➢ Memorandum and Articles of Association (MoA and AoA) ➢ PAN Card/Form 60 ➢ A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf ➢ Name of Persons holding Senior Management position

Sr. No	Type	Type of Documents or the equivalent e-documents to be collected from the customer
		➢ Registered office and Principal place of business if both are different. ➢ Such other documents in respect of the nature of business and financial status of an entity.
5.	Trust	In addition to the documents mentioned in point no. 1, relating to trustees, managers, officers or employees, beneficial owner or authorized signatories or holders of PoA to transact on its behalf. **Certified copy of all the below documents**; ➢ Registration certificate ➢ Trust deed ➢ PAN Card or Form 60. ➢ List of beneficiaries, trustees, settlor, protector, if any and authors of the trust. ➢ the address of the registered office of the trust; ➢ Such other documents in respect of the nature of business and financial status of an entity. ➢ Declaration from Trustee regarding their status while carry out each transaction.
6.	Unincorporated Association/ Unregistered trusts/partnership firms or a body of individuals	In addition to the documents mentioned in point no. 1, relating to beneficial owner, managers, officers or employees, or authorized signatories or holders of PoA to transact on its behalf; ➢ Resolution of the managing body of such association or body of individuals ➢ PAN Card or Form 60. ➢ Power of attorney granted to transact on its behalf and PAN of the persons holding an attorney to transact on its behalf and any OVD for identity and address proof and one recent photograph of such persons. ➢ Such other documents in respect of the nature of business and financial status of an entity.
7.	Person purports to act on behalf of juridicial person or individual or trust. Specifically, not covered such as societies, universities and local bodies like village panchayats	Certified copy of all the below documents or the equivalent e-documents thereof; ➢ Document showing the name of the person authorised to act on behalf of the entity; ➢ Documents, as specified in Section 16, of the person holding an attorney to transact on its behalf and ➢ Such documents as may be required by the Company to establish the legal existence of such an entity/juridical person.

Sr. No	Type	Type of Documents or the equivalent e-documents to be collected from the customer
		➢ Such other documents in respect of the nature of business and financial status of an entity

The company may accept such other documents from the customer in addition to the above-mentioned documents to satisfy and establish the legal existence of such an entity/person. Such a list of documents shall be approved by the Head of -Operations.

8.2 Customer Due Diligence (CDD in case of the Individual, Beneficial Owner, Authorized Signatory and the Power of Attorney Holder.

Sr. No	Name of Documents or equivalent e-documents	Type of Verification
1.	Permanent Account Number	Verify the PAN details with the issuing authority
2.	Submission and Proof of possession of Aadhaar number where offline verification can be carried out.	The Company shall carry out offline verification as per Section 8A of the Aadhaar (Targeted Delivery Of Financial And Other Subsidies, Benefits And Services) Act, 2016.
3.	Where offline verification cannot be performed; Proof of possession of Aadhaar Number, or Passport, Driving Licence, Voter's Identity Card, Job card issued by NREGA , Letter issued by the National Population Register ("OVD")	The Company shall carry out verification through **Digital KYC** as specified under **Annex I**.
4.	Any equivalent e-document of any OVD containing the details of identity and address.	The Company 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 as specified under **Annex I (Digital KYC).**

8.3 Identification of Beneficial Ownership (BO).

Before onboarding a customer, who is not a natural person (i.e., non-individual), the Company shall identify the beneficial owner(s) and verify the beneficial owner's identity.

Nature of Customer	Beneficial Owner of the Entity	
Company	Natural person who, whether acting alone or together, or through one or more Person purports to act on behalf of a juridical person or individual having controlling	Controlling ownership interest" means ownership of or entitlement to more than **10%** of

Nature of Customer	Beneficial Owner of the Entity	
	ownership interest or who exercise control through other means.	shares or capital or profits of the company; "Control" shall include the right to appoint the 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;
Partnership Firm	Natural person who, whether acting alone or together, or through one or more Person purports to act on behalf of a juridical person have ownership or entitlement or who exercises control through other means.	Ownership of entitlement to more than **10%** of capital or profits of the partnership;
Unincorporated Association or Body of Individuals	Natural person who, whether acting alone or together, or through one or more judicial person have ownership or entitlement of unincorporated association or body of individual	Ownership of or entitlement to more than 15% of the property or capital or profits of such association or body of individuals
Trust	Natural person exercising ultimate effective control over the trust through a chain of control or ownership	Trust, Trustee or beneficiaries having 10% or more interest.
where no natural person is identified	the beneficial owner is the relevant natural person who holds the position of Senior Management officials;	
Where the customer the beneficial owner is an entity listed on a stock exchange or it is a subsidiary of such listed entities.	it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.	

In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting shall be obtained.

9 ACCOUNTS OPENED USING AADHAAR OTP BASED E-KYC, IN NON-FACE-TO-FACE MODE:

9.1 The Company will open an Aadhaar OTP base account subject to the following due diligence:

a) The Company will obtain specific consent before onboarding the customers through an Aadhaar registered number only
b) Only term loans will be sanctioned to the customer. The aggregate amount of the term loans sanctioned shall not exceed Rs. 60,000 per year.
c) The account onboarded using OTP based e-KYC shall be operative for 1 year only unless the KYC is performed as per the CDD procedure mentioned in point no. 10 or as per V-CIP. If Aadhaar details are used under VCIP the process shall be followed in its entirety including fresh Aadhaar OTP authentication.
d) In case CDD procedure as mentioned in point no. (c) is not completed within a year. The account shall not be renewed and closed and no further disbursement shall be allowed.
e) The Company will obtain a declaration to the effect that no other account has been opened nor the customer will open other account using OTP based KYC in non-face-to-face mode. Further, while uploading KYC information to CKYCR, the Company will clearly indicate that accounts are opened using OTP based e-KYC and other RE shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.
f) The aggregate balance of all the deposit accounts of the customer shall not exceed Rs. 1,00,000. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD as mentioned at (c) above is complete.
g) The aggregate of all credits in a financial year, in all the deposit accounts taken together, shall not exceed Rs. 2,00,000.
h) Company shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above mentioned conditions.

As risk mitigating measure for an Aadhaar OTP based account, the transaction alerts, OTP, etc., will be sent only to the registered mobile number associated with the Aadhaar card. The customer shall not be allowed to change the mobile number unless the mobile number is registered with Aadhaar.

9.2 In case the customer is not able to produce documents as mentioned in clause no 8, the Company may onboard the customer subject to the following conditions:

a) The Company will obtain a self-attested photograph from the customer.
b) The designated officer of the Company has to certify under his signature that the person onboarded has affixed his signature or thumb impression in his presence.
c) The account shall remain operational initially for a period of 12 months, within which CDD as per clause no 8 shall be carried out.
d) Balances in these accounts taken together shall not exceed Rs. 50,000 at any given point of time.
e) The total credit in all the accounts taken together shall not exceed Rs. 1 Lakh in a year and shall be made aware to do a full KYC account. In case the account is not fully KYC complied no further transaction is allowed in the account.

f) The customer shall be notified when the limit reaches Rs. 40,000 or the total credit in a year reaches Rs. 80,000 that appropriate documents for conducting the KYC to be submitted otherwise no further credit will be provided and the account shall be stopped.

g) KYC verification once done by one branch/office of the Company shall be valid unless its not due for periodic updation.

h) The account shall be monitored and when there is suspicion of ML/TF activities or other high-risk scenarios, the identity of the customer shall be as per CDD procedure.

10 CDD PROCEDURE AND SHARING KYC INFORMATION WITH CENTRAL KYC RECORDS REGISTRY (CKYCR).

a) The Company will capture customer KYC records and upload on the CKYCR portal within 10 days of the commencement of onboarding the customer as per KYC templates for 'Individuals' and 'Legal Entities' (LEs) issued by CERSAI.

b) Once the KYC Identifier is generated by CKYCR, the Company will communicate the same to the individual/LE.

c) In case the customer submit the KYC Identifier for establishing an account-based relationship then the Company will obtain explicit consent from the customer to download/retrieve records from the CKYCR using the KYC identifier.

d) The customer will not be required to submit the same KYC record or information unless;

- there is a change in the information of the customer as existing in the records of CKYCR;
- the current address of the customer is required to be verified;
- the validity period of documents downloaded from CKYCR has lapsed;
- the Company considers it necessary to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer; and
- the KYC record or information retrieved is incomplete or is not applicable as per KYC policy.

e) The Company shall update any additional information or document if any received from the existing customers within 7 days in CKYCR records.

11 V-CIP.

The Company may use and carry out customer due diligence using V-CIP as per Annex- II for onboarding new customers and conversion of existing accounts open in non-face to face mode using Aadhaar OTP based e-KYC authentication as per Section 17 of KYC Master direction issued by the RBI;

- Individual customers,
- Proprietor in case of proprietorship firm,
- Authorized signatories and Beneficial Owners (Bos) in the case of Legal Entity (LE) customers.
- Updation/Periodic updation of KYC for eligible customers

12 ON-GOING DUE DILIGENCE/UPDATION/PERIODIC UPDATION OF KYC.

The Company has adopted a risk-based approach for ongoing due diligence/periodic updation of KYC of the customer. The company will ensure that the information, and data collected under CDD measure and KYC shall be kept up to date as per risk categorisation.

The ongoing due diligence of customers shall include customers' business and risk profile, and the source of funds/wealth to ensure that their accounts are consistent with their knowledge about the customers.

A periodic review of risk categorization of accounts shall be done at least half yearly for application for enhanced due diligence measures. The Company may consider obtaining a recent photograph, requirement for physical presence of the customer, requirement of periodic updation of KYC only in the branch where the credit facility is obtained or a more frequent periodicity of KYC updating than the minimum specified in the policy. Also, the high risk accounts should be more intensively monitored.
The periodic updation will be carried out at least once in every two years for high-risk customers, once in every eight years for medium-risk customers and once every ten years for low-risk customers.

Entity	Criteria	Documents for periodic updation.
Individual Customers	No change in KYC information	a self-declaration will be obtained through a registered email ID, mobile number, or letter in this regard.
	Change in address	a self-declaration of the new address will be obtained through a registered email ID, mobile number or letter and the declared address shall be verified through positive confirmation within two months, by means such as an address verification letter, contact point verification, deliverables etc. or a copy of OVD or the equivalent e-documents thereof for the purpose of proof of address
		Aadhaar OTP based e-KYC in non-face to face mode may be used for updation/periodic updation. The Company shall 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.
Other than Individual	No change in KYC information	a self-declaration will be obtained through a registered email ID, letter from an official authorised along with a Board resolution. The Company shall also obtain fresh Beneficial Owner (BO) information and update the record.
	Change in KYC information	The company shall undertake the KYC process equivalent to that applicable for onboarding a new customer.

In addition to the above, the Company shall ensure that

- If KYC documents are not as per the current CDD standard, then the KYC documents of the customer is as per the current CDD standards shall be obtained, even if there is no change in the customer information.
- PAN details shall be verified from the database of the issuing authority at the time of periodic updation of KYC
- The Company shall provide an acknowledgment for receipt of any documents/letter for KYC updation and the record shall be promptly updated in the system mentioning the date of KYC updation.
- The customer can provide their updated KYC information directly with our Branches or at the central office with the Operation Department.

13 ENHANCED AND SIMPLIFIED DUE DILIGENCE.

The Company is primarily engaged in MSME finance. It does not deal with such a category of customers who could pose a potentially high risk of money laundering, terrorist financing or political corruption and are determined to warrant enhanced scrutiny. The Company also does not open account or provide credit facilities to minors.

13.1 For non-face-to-face customer onboarding (other than customer onboarding using Aadhar OTP base account)

The non-face-to-face customer onboarded by the Company (i.e. the customer without meeting the customer physically or through V-CIP). This includes the use of digital channels such as CKYCR, DigiLocker, equivalent e-document, etc., and non-digital modes such as obtaining a copy of OVD certified by additional certifying authorities. Following EDD measures shall be undertaken by the Company for non-face-to-face customer:

a) The Company shall at first option provide a V-CIP facility if introduced for onboarding the remote customer.
b) In order to prevent fraud, the Company shall not link alternate mobile numbers post CDD with such accounts for transaction OTP, transaction updates, etc. Any revision or new application of credit facility shall be permitted only from the mobile number used for onboarding.
c) Apart from obtaining the current address proof, the Company shall verify the current address through positive confirmation before onboarding or operations in the account. Positive confirmation may be carried out by means such as an address verification letter, contact point verification, deliverables, etc.
d) The Company shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.
e) First transaction in such accounts shall be a credit from the existing KYC-complied bank account of the customer.
f) 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 a face-to-face manner or through V-CIP.

13.2 Accounts of Politically Exposed Persons (PEPs)

If the customer or beneficial owner (including family members and close associates) is a Politically Exposed Person, the Company shall perform additional due diligence measures as mentioned below;

a) The Company shall take additional information and documents concerning to the source of funds and wealth of the PEP and its relative.
b) Any sanction to grant a credit facility to PEP shall be approved by the Board of Directors only.
c) Sufficient information including information about the sources of funds and accounts of family members and close relatives is undertaken wherever possible;
d) all PEP accounts will be subjected to enhanced monitoring on an ongoing basis;
e) in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, committee or board level approval is obtained to continue the business relationship.

14 RISK MANAGEMENT.

The Company follows a Risk based approach for all doing customer assessments. The Company is serving to MSME sector and provides various types of credit facilities. The Company categories all its customers sourced by its branches under low risk because of the nature of the customer, product profiles, customer business and ticket size under which the Company product and policy operates.

The Company categorized all the customer profile into low, medium and high risk based on their profile.

The risk categorization will be based on the following parameters:

a) Customer's identity;
b) Social/financial status;
c) Nature of business activity;
d) business information and their location;
e) geographical risk covering customers as well as transactions;
f) type of products/services offered;
g) delivery channel used for delivery of products/services;
h) types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, and
i) Ability of the customers to confirm identity documents through online or other services offered by issuing authorities.
j) Customer's identity: the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

Indicative List of Risk Categorization

Low Risk Category

Individuals (other than High Net Worth) and entities whose identities and sources of income/fund can be easily identified and transactions in whose accounts by and large conform to the known profile and are not covered in any of the below two categories, shall be categorized as low risk.

The MSME enterprise is entities of modest mean and lies at the bottom of the economy or into the non-formal sector. Most of their turnover might be conducted in cash. However, for PML and AML purview the same shall be categorized as low risk due to the small aggregate transaction.

Low risk customers include customers or entities operating in industry segments not mentioned under the negative list/caution profiles as per the credit policy.

Medium Risk Category

Customers who are likely to pose a higher than average risk may be categorized as a medium or high risk depending on the customer's background, nature and location of the activity, country of origin, sources of funds and customer profile, etc.

Medium-risk customers or entities who are listed in the negative list/caution list profile as per credit policy.

High Risk Category.

Customers who are likely to pose high risk require a higher level of monitoring due to their customer profile or the nature of their business or the location of such customer.

The High-Risk Customers are;

The non-face-to-face to face customers,

- Non-profit Organization or Section 8 Companies
- Politically Exposed Person.
- Persons having dubious reputation as per public information available, etc.
- Firms with ‘sleeping partners’,
- Customers requesting for frequent change of address/contact details
- Sudden change in the loan account activity of the customers
- Frequent closure and opening of loan accounts by the customers
- Negative list issue by RBI, Government and Internal Agency

The Company shall undertake ongoing due diligence and monitoring of high-risk customers to ensure that their transactions are consistent with Company knowledge.

15 RECORD MANAGEMENT AND RETENTION.

The Company shall take the following steps regarding maintenance, preservation, and reporting of customer account information, regarding provisions of the PML Act and Rules:

a) The Company shall maintain all records of the transaction between the Company and the customer for at least 5 years from the date of the transaction.
b) The company shall preserve the identification/address documents of the customer for a period of 5 years after the business relationship is ended.
c) The Company will 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.
d) The Company shall maintain all the information and a record of transactions as prescribed under the Prevention of Money Laundering Rule 3 including the following:

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

15.1 Maintenance of records of transactions (nature and value) as per Rule 3 of PML (Maintenance of Records) Rules 2005:

a) All cash transactions of the value of more than Rs.10 lakhs or its equivalent in foreign currency.
b) All series of cash transactions integrally connected to each other which have been individually valued below Rs.10 lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds Rs.10 lakhs or its equivalent in foreign currency.
c) All transactions involving receipts by non-profit organizations of value more than Rs. 10 lakh, or its equivalent in foreign currency
d) 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.
e) All suspicious transactions whether or not made in cash.
f) all cross-border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of the fund is in India;
g) all purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity, as the case may be.
h) Receipt of Rs. 2 Lakhs or more in cash from a person in a single day or in respect to single transactions as per section 269ST of Income Tax, 1961.

The Company shall maintain records of the identity and address of their customer, and records in respect of the above transactions in hard or soft format.

16 REPORTING REQUIREMENTS TO FINANCIAL INTELLIGENCE UNIT – INDIA.

The Company will be furnished to the Director, Financial Intelligence Unit-India (FIU-IND), information referred in Rule 3 of the PML (Maintenance of Records) Rules, 2005.

a) The Principal Officer of the Company will furnish the cash transaction report (CTR) in the prescribed format with respect to transaction referred clauses (A), (B), (BA), (C) and (E) of sub-rule (1) of rule 3 by 15th of every succeeding month.
b) The Principal Officer of the Company will furnish the Suspicious Transaction Report (STR) in the prescribed format with respect to the transaction referred to in clause (D) of sub-rule (1) of PML Rule 3, Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005, within 7 working days after arriving at the conclusion that the transaction is suspicious.
c) The Principal Officer of the Company will furnish the information in the prescribed format with respect to transaction clause (F) of sub-rule (1) of rule 3, 15th of the every succeeding the quarter.
d) The Company shall deploy robust software which is capable (i) of throwing alerts when the transactions are inconsistent with risk categorization, (ii) updated profile of the customers will be put into use as a part of effective identification and reporting of suspicious transactions.

17 UNIQUE CUSTOMER IDENTIFICATION CODE (UCIC).

Every customer is provided with a unique customer ID. This helps to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable the organization to have a better approach to risk profiling of customers.

18 SELLING OF THIRD-PARTY PRODUCTS.

The Company acting as an agent while selling third party products shall comply with the following directions;

- If the transaction value is above Rs. 50,000, the identity and address of the walk-in customer will be verified by the Company.
- The Company shall maintain complete records of the third-party product.
- The Company shall obtain and verify the PAN given by the account-based as well as walk-in customers.

19 APPOINTMENT OF DESIGNATED DIRECTOR AND PRINCIPAL OFFICER

Mr. Pravash Dash Managing Director & CEO is the designated director who is responsible for ensuring overall compliance as required under the PML Act and the rules.

Mr. Kunal Mehta, Executive Director is designated as the Principal Officer who shall be responsible for monitoring and reporting of all transactions and sharing of information to FIU-IND.

The Company shall communicate to the FIU IND and the Reserve Bank of India if any changes the officer with name, designation, address, and contact details.

Senior Management shall be defined as per the HR policy of the Company.

20 REQUIREMENTS/OBLIGATIONS UNDER INTERNATIONAL AGREEMENTS - COMMUNICATIONS FROM INTERNATIONAL AGENCIES.

The Company shall ensure that it does not have any account i.e credit facility sanction in the name of individuals and entities appearing in the negative or suspective list sanction or issued under the following Acts, Regulators, and Agencies are as under:

The Company shall ensure details of such account resembling to it shall be reported to FIU-IND including transaction details, particular of funds, financial assets, etc. The Company shall not open an account if such a name appears in the list.

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

In terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 as amended from time to time, the Company does not have any account in the name of individuals/entities which are approved by and periodically circulated by the United Nations Security Council (UNSC). The details of the two lists are as under:

a) The "ISIL (Da'esh) &Al-Qaida Sanctions List", established and maintained under Security Council resolutions 1267/1989/2253, which includes names of individuals and entities associated with the Al-Qaida is available at **https://scsanctions.un.org/ohz5jen-al-qaida.html**

b) The "Taliban Sanctions List", established and maintained pursuant to Security Council resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban is available at https://scsanctions.un.org/3ppp1en-taliban.htm

20.2 Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007

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

In case the customer name and entities matches the above, the Company shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO) i.e FIU-IND, designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. A copy of the communication shall be sent to the State Nodal Officer of the RBI.

20.4 UNSCR 1718 Sanctions List of Designated Individuals and Entities, as available at https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm

20.5 Other International Laws and Regulations.

20.5.1 EU Consolidated list of persons, groups and entities subject to EU financial sanctions.: https://data.europa.eu/data/datasets/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions?locale=en

20.5.2 World Bank Listing of Ineligible Firms and Individuals: https://www.worldbank.org/en/projects-operations/procurement/debarred-firms

20.5.3 OFAC Specially Designated Nationals And Blocked Persons List and consolidated List: https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists
https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list-non-sdn-lists

21 HIRING OF EMPLOYEES AND EMPLOYEE TRAINING.

The Company shall undertake an adequate screening mechanism as an integral part of their personnel recruitment/hiring process and conduct ongoing employee training programs that the employees are adequately trained in KYC/AML policy.

ANNEX – I DIGITAL KYC PROCESS

1. The Company is in the process of making available digital KYC applications (apps/software) at customer touch points for undertaking the KYC of the customers. The same should be undertaken only through an authenticated application of the Company.
2. The access of the application will be controlled by the Company and shall not be used by unauthorized persons. The access of the application will be only through login-id and password or Live OTP or Time OTP controlled mechanism given to authorized officials.
3. For KYC the customer should visit the Company office/branch or location of the authorized official or vice-versa. The original OVD should be in possession of the customer.
4. Live photograph of the customer should be taken by the authorized officer and the same photograph should be embedded in the Customer Application Form (CAF). The application should add a watermark in readable form having the CAF number, GPS coordinates, authorized official's name, unique employee code and Date (DD:MM: YYYY) and time stamp (HH:MM: SS) on the captured live photograph of the customer.
5. The application should have the feature that only a live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing the live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.
6. Live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out should be placed horizontally and should be captured vertically from above and water-marking in readable form as mentioned in the above point.
7. No skew or tilt in the mobile device should be there while capturing the live photograph of the original documents.
8. The live photograph of the customer and original documents should be captured in the proper light such that its clearly readable and identifiable.
9. All the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details may be auto-populated by scanning the QR code instead of manual filing the details.
10. Once the above mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to the customer's own mobile number.
11. Upon successful validation of the OTP, it will be treated as a customer signature on CAF. In case the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF.
12. In no case the mobile number of authorized officers shall not be used for customer signature. The Company should ensure that the mobile number used in the customer signature shall not be the mobile number of the authorized officer.
13. Authorized officer shall provide a declaration about the capturing of the live photograph of the customer and the original document. The authorized official should be verified with a One Time Password (OTP) which should be sent to his/her mobile registered number. Upon successful OTP validation, it should be treated as an authorized officer's signature on the declaration.

14. The live photograph of the authorized official shall also be captured in this authorized officer's declaration. Subsequent to all these activities, the Application should give information about the completion of the process and submission of the activation request to the activation officer and generate the transaction-id/reference-id number of the process.
15. The authorized officer should intimate the details regarding the transaction-id/reference-id number to the customer for future reference.
16. The authorized officer should check and verify that:- (i) the information available in the picture of the document is matching with the information entered by the authorized officer in CAF. (ii) live photograph of the customer matches with the photo available in the document.; and (iii) all of the necessary details in CAF including the mandatory field are filled properly.
17. On Successful verification, the CAF shall be digitally signed by an authorized officer who will take a print of CAF, get signatures/thumb-impression of the customer at the appropriate place, the scan copy shall be upload the same in the system. Original hard copy may be returned to the customer.

ANNEX – II: VIDEO BASED KYC PROCESS (V-CIP)

1. V-CIP Infrastructure

1.1. The technology infrastructure for V-CIP shall be housed in the Company own premises and the V-CIP connection and interaction should be originate from the Company own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines. Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with the Company only and all the data including video recording is transferred to the RE's exclusively owned/leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the RE.

1.2. The Company infrastructure should ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.

1.3. The V-CIP infrastructure/application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.

1.4. The video recordings should contain the live GPS coordinates (geo-tagging) of the customer undertaking the V-CIP and the date-time stamp. The quality of the live video in the V-CIP should be adequate to allow identification of the customer beyond doubt.

1.5. The application should have components with face liveness/spoof detection as well as face-matching technology with a high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the RE. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

1.6. Based on experience of detected/attempted/'near-miss' cases of forged identity, the technology infrastructure including application software as well as work flows should be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber event under extant regulatory guidelines.

1.7. The V-CIP infrastructure should undergo necessary tests such as Vulnerability Assessment, Penetration testing, and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by the empanelled auditors of the Indian Computer Emergency Response Team (CERT-In. Such tests should also be carried out periodically in conformance to internal/regulatory guidelines.

1.8. The V-CIP application software and relevant APIs/webservices should also undergo appropriate testing of functional, performance, maintenance strength before being used in a live environment. Only after the closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

2. V-CIP Procedure

2.1. The Company should formulate a clear work flow and standard operating procedure for V-CIP. The V-CIP process should be operated only by specially trained officials of the Company.

2.2. In case there is a disruption of any sort including pausing of video, reconnecting calls, etc., should not result in the creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then there is no need to initiate a fresh session by the RE. However, in case of call drop/disconnection, fresh session shall be initiated.

2.3. To establish that the interactions are real-time and not pre-recorded, the sequence and/or type of questions, including those indicating the liveness of the interaction, during video interactions shall be varied.

2.4. If any prompting is observed at the end of the customer, the application should reject the process of KYC.

2.5. The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at the appropriate stage of workflow.

2.6. The authorized official of the Company who is performing the V-CIP should record audio-video as well as capture a photograph of the customer present for identification and obtain the identification information using any one of the following:

- OTP based Aadhaar e-KYC authentication
- Offline Verification of Aadhaar for identification
- KYC records downloaded from CKYCR, in accordance with Section 56, using the KYC identifier provided by the customer
- Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker.
- RE shall ensure to redact or blackout the Aadhaar number in terms of Section 16.
- In case of offline verification of Aadhaar using an XML file or Aadhaar Secure QR Code, the Company should ensure that the XML file or QR code generation date should not be older than 3 working days from the date of carrying out V-CIP.
- The Company should also complete the V-CIP within 3 working days of downloading/obtaining the identification information through CKYCR/Aadhaar authentication/equivalent e-document.

2.7. In case the address of the customer is different from that indicated in the OVD, suitable records of the current address should be captured. The Company should also ensure that the economic and financial profile/information submitted by the customer should also confirmed from the customer undertaking the V-CIP in a suitable manner.

2.8. Application should capture a clear image of the PAN card displayed by the customer during the process, except where e-PAN is provided by the customer. The PAN details should be verified from the database of the issuing authority including through Digilocker.

2.9. The Company should ensure that use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.

2.10. The authorized official of the Company should ensure that the photograph of the customer in the Aadhaar/OVD and PAN/e-PAN matches with the customer undertaking the V-CIP and the identification details in Aadhaar/OVD and PAN/e-PAN should match with the details provided by the customer.

2.11. All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of the process and its acceptability of the outcome.

3. V-CIP Records and Data Management

3.1. The entire data and recordings of V-CIP should be stored in a system located in India. The Company should ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in the RBI master direction shall be equally applicable for V-CIP.

3.2. The activity log along with the credentials of the official performing the V-CIP shall be preserved.