KYC policy and actual process of Merchant

Aurionpro Payment Solutions Private Limited.

270, Synergia IT Park, Gautam Nagar, MIDC Industrial Area, Rabale, Navi Mumbai – 400 701, India

Tel: +91-22-66172600

Fax: +91-22-66172666

Website: www.auropay.net

Date	Version	Function	Accountable	Change Description
14-09-2024	1.0	Created	Saloni Rai	
15-11-2024	1.0	Reviewed & Approved	Bhakti Zaveri	
21-04-2025	1.1	Updated	Badal Pawar	
28-04-2025	1.1	Reviewed & Approved	Bhakti Zaveri	

Reference Number: AuroPay_KYC_Policy and actual process of mertchant_28042025_v1.1

TABLE OF CONTENTS

Sr. No.	CONTENT	Page No.
1.0	Introduction	4
2.0	Objectives & Key Elements of the Policy	4
3.0	Compliance of AML/KYC Policy	4
4.0	Appointment of Key Personnel	5
5.0	Definitions	6
6.0	Merchant Acceptance Policy	9
7.0	Merchant Identification Procedure	9
8.0	Required KYC Due Diligence	10
9.0	Monitoring of Transactions	14
10.0	Records Retention	14

11.0	Reporting of Suspicious Transactions	14
12.0	Risk Management	15
13.0	Training	16
14.0	Risk Assessment of Money Laundering and Terrorist Financing	16
15.0	Secrecy Obligations	16
16.0	CKYCR Compliance	17
17.0	Adoption of New Technologies	17
18.0	General	18
19.0	Appendix I – Document Checks	19
20.0	Appendix II – Restricted Merchant Category	21

Policy on Know Your Customer (KYC) & Anti -Money Laundering (AML) Standards

1.0. INTRODUCTION:

AuroPay's Policy on Know Your Customer (KYC) & Anti-Money Laundering (AML) Standards (**the "Policy"**) has been framed in accordance with the Reserve Bank of India (RBI) Master Direction – Know Your Customer (KYC) Direction, 2016 (KYC Master Directions), as amended from time to time and the terms of the provisions of Prevention of Money Laundering Act (PMLA), 2002 and the Prevention of Money Laundering (Maintenance of Records) Rules (PMLR), 2005, as amended from time to time by the Government of India as well as rules and regulations made thereunder. In line with the said guidelines, this Policy details the minimum standard for AuroPay with regard to the Merchant identification procedures and conduct Merchant due diligence while undertaking a transaction by establishing an account-based relationship and monitoring their transactions in accordance the provisions of the aforementioned Act, Rules. Merchant Due Diligence is created to help payment service providers and other financial institutions such as banks to verify if the Merchant are who they say they are, confirm that they are not on any list that prohibits to provide services to them and to assess their risk factors. Conducting due diligence is an important tool to avoid money laundering and the financing of terrorism. It is also essential that AuroPay knows with whom it is doing business in order to guarantee ethical operational management and to maintain a good reputation and thereby the trust of stakeholders.

Failure to carry out AML measures such as KYC could lead to sanctions from regulators, loss of the license to operate, reputational damage and to financial loss. In view of the same, the Board of Directors of **AURIONPRO PAYMENT SOLUTIONS PVT. LTD.** ("**Aurionpro Payments**," "**the Company**," "**AuroPay**") has adopted this Policy framework on Anti-Money Laundering (AML) – Know Your Customer (KYC) measures in line with the RBI guidelines.

The Company will adopt the best practices prevalent and as prescribed by RBI from time to time and will make suitable modifications, if any, necessary to this Policy to conform to the applicable standards. This Policy is applicable across all business segments and employees of the Company and is to be read with any operational guidelines issued sometimes. This document is a living document and will be reviewed and updated at least annually or as and when necessitated. Any amendments arising from such reviews will be incorporated into the Policy following approval by the Board of Directors.

2.0. OBJECTIVES & KEY ELEMENTS OF THE POLICY:

(a) To put in place systems and process to control financial frauds, identify money laundering activities and safeguarding the Company against any illegal or criminal activity;

(b) To build a system and procedures for Merchant identification and verifying his / her identity and residential address; and

(c) To monitor transactions of a suspicious nature;

(d) To ensure that the concerned staffs are satisfactorily trained in AML, KYC, and Counter Financing Terrorism (CFT) procedures; and

(e) To comply with applicable laws and regulatory guidelines.

The Policy includes seven (7) key elements:

1. Merchant Acceptance Policy (MAP);

2. Merchant Identification Procedures (MIP);

3. Monitoring of Transactions;

4. Records Retention;

5. Reporting of Suspicious Transactions;

6. Risk Management; and

7. Training.

3.0. COMPLIANCE OF AML/KYC POLICY

(a) The Company ensures compliance with the AML/KYC Policy through:

(i) Specifying 'Senior Management' for the purpose of AML/KYC compliance.

(ii) Assigning role to Senior Management for effective implementation of policies and procedures.

(iii) Independent evaluation of the compliance functions, policies, and procedures, including legal and regulatory requirements.

(iv) Concurrent/internal audit system to verify the compliance with KYC/AML policies and procedures.

(v) Submission of audit notes and compliance to the Audit Committee.

(b) The Company does not outsource the decision-making functions regarding compliance of AML/KYC norms.

4.0. Appointment of Key Personnel

AuroPay will appoint a Principal Officer and a Designated Director to ensure full compliance with the provisions of the KYC Master Directions, the PMLA, and the PMLR. These roles will be assigned to separate individuals to maintain functional independence and accountability.

AuroPay will formally communicate the names, designations, office addresses, and contact details of both the Principal Officer and the Designated Director to the FIU-IND and the RBI.

- **Principal Officer**

  The Principal Officer will be responsible for:

  - Ensuring AuroPay's compliance with all applicable laws, regulations, and guidelines related to KYC/AML/CFT.

  - Establishing and managing a robust transaction monitoring system to detect, investigate, and report suspicious transactions.

- Liaising with regulatory and enforcement authorities, including FIU-IND, and providing timely, accurate, and complete information as required under applicable legal and regulatory frameworks.

- **Designated Director**

The Designated Director will assume full responsibility for overseeing and ensuring AuroPay's comprehensive compliance with all regulatory requirements related to KYC,/AML/CFT. This mandate will include strict adherence to the provisions of the PMLA and the PMLR, as updated from time to time.

5.0. DEFINITIONS

i. **"Aadhaar number"** means an identification number issued to an individual by Unique Identification Authority of India (UIDAI) on receipt of the demographic information and biometric information as per the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 as amended from time to time. In terms of the Aadhaar Act, every resident shall be eligible to obtain an Aadhaar number. Aadhaar will be the document for identity and address.

ii. **"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.

iii. **"Authentication",** as defined under sub-section (c) of **Section 2** of the Aadhaar Act, means the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted to the Central Identities Data Repository (**CIDR**) for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it;

iv. **"Beneficial Owner (BO)"** shall mean

a. Where the Merchant is a company: BO is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest[1] or who exercise control[2] through other means.

b. Where the Merchant is a partnership firm: BO is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10 percent of capital or profits of the partnership or who exercises control through other means.

c. Where the Merchant is an unincorporated association or body of individuals: BO is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 percent of the property or capital or profits of the unincorporated association or body of individuals[3].

---

[1] Controlling ownership interest" means ownership of/entitlement to more than 10 percent of the shares or capital or profits of the company.

[2] "Control" will include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

[3] Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

d. **Where the Merchant is a trust:** BO will include identification of the author of the trust, the trustee, the beneficiaries with 10 percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

v. **"Biometric information,"** means photograph, fingerprint, Iris scan, or such other biological attributes of an individual as specified under Aadhaar (authentication) regulations;

vi. **"Central Identities Data Repository" (CIDR),** means a centralized database at one or more locations containing all Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other related information;

vii. **"Central KYC Records Registry" (CKYCR)** means an entity defined under **Rule 2(1) (aa)** of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a Merchant.

viii. **"Customer"** means the end user of the services provided by the Merchants with whom the Company has entered into an arrangement for providing PA.

ix. **"Demographic information,"** includes information relating to the name, date of birth, address, and other relevant information of an individual, as may be specified by regulations for the purpose of issuing an Aadhaar number, but shall exclude sensitive personal information of an individual;

x. **"Designated Director"** means a person designated by the Company to ensure compliance with the obligations imposed under the PML Act and the Rules.

xi. **"Enrolment number"** means a 28-digit Enrolment Identification Number allocated to an individual at the time of enrolment of Aadhaar.

xii. **"E-KYC authentication facility"** means authentication facility in which the biometric information and/or OTP and Aadhaar number securely submitted with the consent of the Aadhaar number holder through a requesting entity, is matched against the data available in the CIDR, and the Authority returns a digitally signed response containing e- KYC data;

xiii. "**Key Controller**" means members of a group of persons chosen to control or govern the affairs of a legal entity:

- *For a corporate entity:* key controllers are those natural persons who have the position of CEO, CFO or director who is authorized to act on behalf of the Merchant;
- *For a partnership:* key controllers are all managing partners and other persons authorized to manage (and act on behalf of) the partnership.

xiv. **"Identity information"** in respect of an individual, includes individual's Aadhaar number, biometric information and demographic information;

xv. **"Officially Valid Document" (OVD)** means a) the Aadhaar Card, b) the passport, c) the driving license, d) the Voter's Identity Card issued by the Election Commission of India, e) job card issued by NREGA duly signed by an officer of the State Government, f) letter issued by the National Population Register containing details of name and address.

xvi. **"Person"** has the same meaning assigned in the Act and includes a. an individual, b. a company, c. a firm, d. an association of persons or a body of individuals, whether incorporated or not and e. any agency, office or branch owned or controlled by any of the above persons.

xvii. **"Principal Officer"** means an officer at the management level official nominated by the Company responsible for activities as specified under this Policy.

xviii. **"Resident,"** means an individual who has resided in India for a period or periods amounting in all to one hundred and eighty-two days or more in the twelve months immediately preceding the date of application for enrolment for Aadhaar

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 suspicious or unjustified circumstances; or c. appears to not have economic rationale or bona-fide purpose; or d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

xvii "Transaction" means a purchase, or a sale made and includes: a. opening of an account and b. transfer of funds by electronic means.

xviii. Merchant" means an individual or legal entity(ies), based in India, with whom the Company has entered into a contract (Merchant Agreement) for the purpose of providing PA services.

xix."Merchant Due Diligence (MDD)" means identifying and verifying the Merchant and the ultimate beneficial owner during onboarding and reviewing. MDD consists of:

- Collection of information about the Merchant and thereby investigating whether the Merchant is who he says that he is.
- Risk assessment plus risk classification of each Merchant. Depending on the risk factor

due diligence can require an enhanced, standard, or simplified due diligence. **xx. Merchant identification"** means undertaking the process of MDD.

xxi. "Group" has been defined in line with that of Income Tax Act which shall mean entities which are required to be consolidated for financial reporting purposes (parents, subsidiaries, associates).

xxii. "KYC Templates" means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.

xxiii. "On-going Due Diligence" means regular monitoring of transactions in accounts to ensure that they are consistent with the Merchant's profile and source of funds.

xxiv. "Periodic Updating" means steps taken to ensure that documents, data, or information collected under the MDD process is up-to-date and relevant by undertaking reviews of existing records.

xxv. "Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States/Governments, senior

politicians, senior government/judicial/military officers, senior executives of state- owned corporations, important political party officials, etc.

xxvi. **"Senior Management"** shall mean officers / personnel of the Company who are members of its core management team excluding Board of Directors and shall comprise all members of Management one level below the Chief Executive Officer / Managing Director / Whole-Time Director including Chief Executive Officer (CEO), in case they are not part of the Board) and shall specifically include Company Secretary and Chief Financial Officer (CFO).

6.0. MERCHANT ACCEPTANCE POLICY ("MAP")

The Merchant Acceptance Policy is developed laying down criteria for acceptance of the Merchants. The Merchant Acceptance Policy shall ensure that guidelines are in place on the following aspects of Merchant relationship in the Company:

a. The Company shall not open any account in anonymous or fictitious name(s).

b. The Company shall not open any account without appropriate Merchant Due Diligence (MDD) measures, either due to non-cooperation of the Merchant or non-reliability of the documents / information furnished by the Merchant.

c. The Company must not link alternate mobile numbers post the conduct of MDD.

d. Transaction or account-based relationship is undertaken by following the proper MDD.

e. For accounts opened using One-Time Password (OTP) based e-KYC process, transactions alerts and OTPs to be sent only to Aadhaar linked mobile numbers.

f. The mandatory information to be sought for KYC purpose while opening an account and during the periodic updating, is specified.

g. Optional / additional information is obtained with the explicit consent of the Merchant after the account is opened.

h. The Company should place suitable system to ensure that the identity of the Merchant does not match with any person or entity, whose name appears in the sanctions lists issued by UN Security Council and / or the Reserve Bank of India (RBI) from time to time.

i. The Company must allot a Unique Merchant Identification Code (**MID**) to all its new and existing relations with its customers.

The Company will ensure that the adoption of MAP and its implementation should not result in denial of services to the public, especially to those who are financially or socially disadvantaged.

7.0. MERCHANT IDENTIFICATION PROCEDURE (MIP)

One of the objectives of the "KYC" norms is to ensure appropriate Merchant Identification. KYC process includes ID card verification, document verification such as utility bills as proof of address, and biometric verification.

The Company's MIP is integrated into the AML (Anti Money Laundering) program for the company in terms of the Prevention of Money Laundering Act, 2002 and the relevant rules notified there under (PMLA), which contains provisions requiring the business processes to: 1. verify the identity of any Person transacting with the Company to the extent reasonable and practicable; 2. maintain records of

the information used to verify a Merchant's identity, including name, address and other identifying information; and 3. consult lists of known or suspected terrorists or terrorist organizations provided to the Company by any applicable government agency to determine whether a person opening an account or an existing Merchant appears on any such list.

The Company will perform appropriate, specific, and where necessary, Enhanced Due Diligence on its Merchants that is reasonably designed to know and verify the identity of its Merchants and to detect and report instances of criminal activity, including money laundering or terrorist financing.

AuroPay will rely on MDD conducted by a third party only when the following conditions are fully satisfied:

- Records or information of the MDD conducted by the third party are promptly obtained from the third party or from the CKYCR.
- Merchant identification data and related MDD documentation will be promptly provided by the third party upon request.
- The third party is regulated, supervised, or monitored to ensure compliance with MDD and record-keeping requirements in accordance with the obligations under the PMLA.
- The third party is not based in a country or jurisdiction assessed as high risk.

Notwithstanding the reliance on a third party, Company will retain ultimate responsibility for MDD and the implementation of EDD measures, as applicable.

8.0. REQUIRED KYC DUE DILIGENCE

MDD process consists of the following steps: (i) identifying the Merchant and verifying the Merchant's identity on the basis of documents, data or information obtained from a reliable and independent source (if it regards a legal entity, identifying the legal entity and its legal representatives and verifying the identities); (ii) identifying the Merchant's ultimate beneficial owner(s) ("**UBOs**") (i.e. the natural persons who own or control the Merchant) and taking reasonable measures to verify their identity; (iii) performing an adverse media and sanctions check on the Merchant, its UBOs and legal representatives, as well as sorting out whether UBOs or legal representatives might qualify as a Politically exposed person ("**PEP**"); (iv) obtaining and, as appropriate, assessing information on the purpose and intended nature of the business relationship; (v) assessing the industry of Merchant (which industry is the Merchant active in); (vi) legal structure of the Merchant. Therefore, accordingly, as per the Reserve Bank of India's **('RBI') KYC Master Direction, the RBI PA Guidelines, and the Prevention of Money Laundering Act, 2002 (the 'PMLA')** (among others), we shall rely on the following six (6) stage process:

Stage 1: Verification through Documents and non-Documentary methods

The first stage involves the collection of KYC documents and their verification process. It can be one or more of the following forms- Individual KYC, Platform KYC, and Business KYC:

Individual KYC: When a Merchant is an individual (e.g.: a sole proprietor), we carry out a 'KYC' process, or MDD for an individual. Broadly, we verify the Merchant's identity via an
'Officially Valid Document' or OVD verification (identity documents like Aadhaar, passport, driving license, etc.), individual PAN verification, and if necessary, current address proof check (utility bills, etc.). We also ask for more documents to verify their financial/business status, subject to explicit consent of the said Merchant.

Business KYC: When a business partner is on board, we carry out a Business KYC process, or MDD for a business. Here we replace the OVD check with an 'entity-proof' check. This differs based on the legal recognition of the entity. For example, if the entity is a company, we need to verify the certificate of incorporation, memorandum and articles of association, its Board of Directors etc. If the entity is a trust/partnership, we need the trust/partnership deed, registration certificates, etc. Once the licensing/registration is verified, we need to ascertain that the officer/employee transacting with us on company's behalf has the authority to do so. For this we need the relevant Board resolutions, power of attorney, etc. Next, we need the Business PAN, and address proof (verified GST) if your licensing/registration documents don't reflect your current address. We also need to conduct '**ultimate beneficial owner**' checks i.e., we need to verify who has actual ownership/control, like the directors, shareholders, etc., and carry out the 'KYC' process separately for them.
We also verify numerous other documents for due diligence processes (discussed below).

Platform KYC:

Besides, the Company may also through non-documentary methods carry out Merchant verification process at its discretion. These methods may include but are not limited to 1. Contacting or visiting a Merchant; 2. Independently verifying the Merchant's identity through other sources; 3. Checking references with other financial institutions; or 4. Obtaining a financial statement.

It is hereby clarified that only such additional information, the requirement of which has not been specified in the KYC requirement of AuroPay, shall be obtained with the explicit consent of the Merchant.

Stage 2: Verification against sanction and PEP lists

Next, we need to verify the names of the Merchants, their ultimate beneficial owners, and legal representatives against certain lists, like national and international terrorist lists, or 'Politically Exposed Persons' ("**PEP**") lists. If a name matches a sanctions list, we need to report this to the Financial Intelligence Unit of India ('**FIU-IND'**) by filing Suspicious Transaction Report (**STR**) without prompting the said Merchant. Along with these, we verify numerous other lists, like blacklists/ Grey lists/ defaulter lists/Alert List for companies, directors, etc. issued by banks, the Reserve Bank of India, the Ministry of Corporate Affairs (MCA), the Securities and Exchange Board of India (SEBI), the Enforcement Directorate (ED), the Office of Foreign Assets Control (U.S.), etc. (for a detailed list please see **Appendix II** below). Besides, we also obtain and assess information on the purpose and intended nature of the business relationship, assessing the industry of the Merchant (which industry the Merchant is active in) as well as the legal structure of the Merchant. These checks aid us in the fight against terrorism and money laundering.

Stage 3: Onboarding policies and Merchant screening

Next, we carry out a background and antecedent check, which takes the form of an initial screening, and for which we define an internal Merchant Onboarding Policy. Our aim here is to verify the nature, purpose and bona fide of a prospective Merchant's business. We conduct a range of checks such as licensing/registration checks, credit checks, profit and loss statement checks, balance sheet reviews, etc., based on information we seek directly from the prospective Merchant, together with checking publicly available information like the Merchant's websites, product listings, end-customer reviews, social media activity, etc., to ascertain business legitimacy. We are also required under law to ascertain whether the Merchants are PCI-DSS compliant.

Stage 4: Merchant profiling and diligence levels

After these initial checks and based on the assessment on the above risk elements including but not limited to geographical risk, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken, etc., we need to classify the Merchants in a certain risk category as low/medium/high risk/unacceptable. Risk categorization determines which level of due diligence needs to be applied. This helps determine how much information about the Merchant needs to be collected and independently verified. In addition, they determine the level of future monitoring. AuroPay shall maintain cconfidentiality with respect to risk categorization and the reasons thereof at all times to avoid tipping off the Merchant. AuroPay has implemented simplified, standard, or enhanced due diligence processes as detailed below.

Due Diligence is performed based on the characteristics of the Merchant, AuroPay is dealing with, and the risk associated with this Merchant. MDD can be simplified, standard or enhanced. Diligence levels and levels of post onboarding monitoring that we carry out are defined based on this. Also, we are prohibited from servicing some businesses altogether (hacking, weapons, etc.), while others are considered high-risk (pharmaceuticals, matrimony, gaming, security brokers, jewelry, etc.) requiring increased monitoring and diligence.

1. ***Simplified Due Diligence (SDD):*** only basic information needs to be collected. SDD applies to Merchants or other parties which can be qualified as or are assessed as being of the risk category "low risk." The verified information can be restricted to the expected frequency of transactions. Stock listed companies and their wholly owned subsidiaries (e.g., 100 % stock listed entity, or 100% subsidiary of stock listed entity) are at lower risk by default, requiring only Simplified Due Diligence (if no other high-risk factors apply to the Merchant)

2. ***Standard Merchant Due Diligence (MDD)*** should be applied on standard-risk Merchants. Privately owned companies and other entities are generally assessed as higher risk than listed companies because they are exposed to a lower level of external scrutiny than those that are publicly owned. Therefore, Standard Merchant Due Diligence needs to be exercised on non-listed companies, associations, etc. For such relationships, subject to the requirements on the local regulations, the identities of the ultimate beneficial owners and legal representatives may be verified in addition to corporate entity verification. Merchants can be categorized as "low" or "medium" risk.

3. ***Enhanced Due Diligence (EDD)*** should be applied to high-risk Merchants. Enhanced due diligence must also be applied to the ultimate beneficial owners or key controllers of high-risk companies or companies with complex structures. For EDD, additional due diligence requirements to the standard Merchant due diligence process must be performed, such as: • Obtaining a copy of a license to operate (e.g.: Forex, Gambling, Cryptocurrency); • Reviewing EDD information daily, and • Incorporate the high-risk elements as part of the Transaction Monitoring. Each business process shall establish appropriate standards, methodology and procedures for conducting Enhanced Due Diligence. The following is the indicative list where the risk perception of a Merchant may be considered higher: i. Merchants requesting frequent change of address/contact details; ii. Sudden change in the activity of the Merchants iii. Frequent closure and opening of accounts by the Merchants; iii. identity of the Customer is not verified in face-to-face manner or through V-CIP, etc. iv. Persons or Beneficial Owners identified as PEPs; v. Merchants classified as high-risk; vi. High account turnover inconsistent with business profile; vii. Suspected involvement in

money laundering, terrorist financing, or unlawful activities; and viii. Onboarding through non-face-to-face channels.

These events call for enhanced due diligence in keeping the account monitored closely for a re-categorization of risk, updating fresh KYC documents, etc., which shall form part of the policies.

AuroPay will obtain additional information and documentation from the Merchant and will implement the following EDD measures:

- Conduct in-depth scrutiny of all transactions associated with the Merchant.
- Assess the customer acquisition process and verify the method used for delivering goods or services.
- Review high-risk accounts on a quarterly basis to ensure ongoing compliance.
- Collect detailed information regarding the sources of funds and overall wealth of the Merchant.
- Verify supporting documents such as proof of goods or service delivery and corresponding invoices.
- Ensure that the first transaction is credited to an existing KYC-compliant bank account held by the Merchant.
- Conduct field verification.
- Establish robust risk management systems to identify whether a Merchant or their beneficial owner qualifies as a PEP. Upon onboarding a PEP, AuroPay will implement the following EDD measures:
    - Conduct thorough assessments to determine the source of funds and overall wealth.
    - Secure formal approval from Senior Management prior to account activation.
    - Apply enhanced and continuous monitoring of the account.
    - In cases where an existing Merchant or their beneficial owner is subsequently identified as a PEP, AuroPay will obtain renewed approval from Senior Management to maintain the business relationship.

Stage 5: Ongoing due diligence

Post onboarding, our due diligence checks will continue to keep track of any changes in Merchant's behavior that are a cause for concern. This is to be achieved by verifying the Merchant data base daily against the various sanctions list specified in the directions and use of Artificial Intelligence (AI) & Machine Learning (ML) has been recommended for complying. For example, a change in Merchant website details or an unexpected listing of high-risk products can indicate fraud. These may also call for re-reviewing Merchant risk profiles and due diligence levels.

Stage 6: Periodic Updates

Lastly, we need to update both Merchant risk profiles and KYC periodically. As per law, we must update Merchant KYC every 10 (low risk), 8 (medium risk) and 2 (high risk) years. The ongoing due diligence checks also aid us with this. For any periodic updating, Aadhaar OTP based e-KYC may be used. However, for any change in address, positive confirmation is not required for OTP based e-KYC. Merchants shall be advised to submit the updated documents in case of any changes within thirty (30) days.

9.0. MONITORING OF TRANSACTIONS

Ongoing monitoring is an essential element of an effective AML/KYC process. Monitoring transactions to be conducted considering the account's risk profile and sensitivity. Aurionpro Payments shall make endeavors to understand the normal and reasonable activity of the Merchant so that the transactions that fall outside the regular/pattern of activity can be identified.

The Company also monitors transactions of a suspicious nature on an on-going basis and ensures that such transactions notified under Section 12 of the PML Act, 2002, are reported to the appropriate law enforcement authority. The extent of monitoring by the Company depends on the risk sensitivity of the account and special attention is given to all complex unusually large transactions.

10.0. RECORDS RETENTION

Aurionpro Payments shall document and implement appropriate procedures to retain records of KYC due diligence and anti-money laundering measures. The Company has the system to (a) maintain all necessary transactional records between the Company and the Merchant, for minimum five (5) years from the date of transaction; (b) preserve the records related to the identification of the Merchants obtained while opening the account and during the course of business relationship, for minimum five (5) years after the business relationship is ended; (c) make immediately available the identification records/updated records and transaction data to the competent authorities upon request. All AuroPay employees involved in the MDD process must be aware of the requirement to retain all MDD related documents and records within set timeframes.

11.0 REPORTING OF SUSPICIOUS TRANSACTIONS

Reporting Requirements to Financial Intelligence Unit – India: Monitoring and screening may lead to the conclusion that there are unusual transactions or suspicious activities that must be reported. This might require collecting further information regarding a Merchant or a transaction before deeming it suspicious. AuroPay implemented a risk-based approach based on - but not limited to - red flags to monitor and report suspicious activity. Some of these red flags are:

- The information received from the Merchant appears to be misleading, not complete or wrongly provided.
- The Merchant’s business profile does not match the transactions that are processed on behalf of the Merchant.
- The Merchant has an agent or financial advisor that acts on behalf of him without the proper documentation, such as a power of attorney.
- The Merchant submits its MDD documentation showing an unclear ownership structure.
- The Merchant submits unusual or suspicious identification documents or declines to provide the originals for verification or declines to provide certain documentation.

- The Merchant is reluctant to reveal details about its business activities or to provide the financial statements.
- The Merchant requests the remittance to be transferred to an offshore bank account.
- Merchants that discuss record keeping or reporting requirements with the intention of avoiding them.

Upon detecting a suspicious transaction during transaction monitoring, AuroPay will initiate a comprehensive investigation into both the Merchant and the transaction in question. If the investigation confirms the transaction as suspicious, the Principal Officer will prepare and submit a detailed STR to the Director of the FIU-IND within a strict timeframe of 7 days.

AuroPay will not impose any restrictions on accounts for which a STR has been filed unless such action is required to fulfill legal obligations. In such instances, AuroPay will take all necessary measures to ensure that the Merchant is not alerted.

AuroPay will strictly prohibit any form of tipping off. Tipping off refers to informing or alerting a Merchant that their account has been, or may be, reported to regulatory authorities or the FIU-IND for suspicious activity. However, requesting information from a Merchant during the course of due diligence will not be considered tipping off.

The Company shall be registered with FIU-IND and shall submit mandatory monthly reports including but not limited to Suspicious Transaction Report (STR) on identification of such transaction with FIU-IND. Additionally, details of Principal Officer (PO) and Designated Directors (DD), must be shared with both the RBI as well as FIU-IND. AuroPay prohibits its employees to disclose the filing of a suspicious activity to the subject of the report or that a possible investigation is initiated.

Information to be preserved: The information that needs to be preserved is the nature of transactions, amount, and the currency in which it was denominated, date of transaction and the parties to the transaction.

12.0. RISK MANAGEMENT

The Board of Directors of the Company will ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It will cover proper management oversight, systems and controls, segregation of duties, training, and other related matters. Responsibility would be explicitly allocated within the Company for ensuring due implementation of the Company's policies and procedures. The Company shall, in consultation with the Board, devise procedures for creating Risk Profiles of their existing and new Merchants and apply various Anti-Money Laundering measures keeping in view the risks involved in a transaction, account or business relationship.

The Company shall have a risk-based approach which includes the following:

a) Merchants shall be categorized as a low, medium, and high-risk category based on the assessment and risk perception of the Company.

b) Merchant risk categorization shall be undertaken based on parameters such as their identity, social / financial status, nature of business activity, information about the Merchant's business and their location, etc.

13.0. TRAINING

Training and educating of all AuroPay's employees is essential to operate and apply the requirements set in this Policy and in the local AML&MDD Programs. The trainings will train and test employees and where needed third parties on various topics such as relevant laws, regulations, AuroPay's policies and procedures and prohibited conduct. AuroPay associate and subsidiaries have a local AML&MDD training program in place that includes local circumstances related to MDD and AML.

14.0 Risk Assessment of Money Laundering and Terrorist Financing

AuroPay will establish a comprehensive, structured assessment framework to proactively address risks related to money laundering and terrorist financing (ML/TF). This framework will include the following key actions:

- Conducting an in-depth evaluation of all pertinent risk factors to determine the overall risk exposure and implementing targeted mitigation strategies.
- Incorporating sector-specific vulnerabilities as identified and communicated by regulatory and supervisory authorities.
- Executing risk assessments that align with the Company's operational scale, geographic footprint, organizational complexity, and business model.

All risk assessments will be thoroughly documented, and their findings will be formally presented to the Board of Directors or a designated Board committee. These records will remain readily accessible to relevant authorities upon request.

The Board or its designated committee will assume full responsibility for determining the frequency of these assessments, with a minimum requirement of conducting them annually.

AuroPay will adopt a risk-based approach to ensure effective mitigation and management of identified ML/TF risks. To support this approach, the Company will implement and maintain a Board-approved Risk Management Policy, along with robust operational processes designed to address these risks comprehensively.

15.0 Secrecy Obligations

AuroPay will uphold the strict confidentiality of all information acquired through its contractual engagements with Merchants. In all instances of data or information requests from government authorities or other agencies, AuroPay will ensure that any disclosure fully complies with applicable legal provisions governing transaction confidentiality.

AuroPay will disclose data or information only under the following exceptional circumstances:

- When legally mandated to do so.
- When there is a legal obligation to inform the public.
- When disclosure is essential to safeguard AuroPay's legitimate interests.
- When the Merchant has provided explicit or implied consent for such disclosure.

16.0 CKYCR Compliance

AuroPay will register with the Central KYC Records Registry (CKYCR) to receive, store, safeguard, and retrieve Merchant KYC records in digital format. AuroPay will ensure full compliance with Master Direction – Know Your Customer (MDD) procedures, including the timely uploading of KYC data to the CKYCR, in strict accordance with the Operational Guidelines issued by CERSAI.

In this regard, AuroPay will take the following actions:

- Capture KYC information using the CERSAI-prescribed templates for both 'Individuals' and 'Legal Entities' (LEs), as applicable, and upload the data to the CKYCR in the format and manner prescribed under the Act and Rules.
- Upload Merchant KYC information within 10 days of establishing an account-based relationship, using the designated CKYCR template.
- Communicate the KYC Identifier generated by the CKYCR to the respective Merchant promptly.
- Retrieve KYC records from the CKYCR using the Merchant's KYC Identifier and request additional documentation from the Merchant when necessary, including but not limited to the following scenarios:
    - Changes in the Merchant's information recorded in the CKYCR;
    - Incomplete or non-compliant KYC records based on current regulatory standards; o

      Expiration of the validity period of downloaded documents;
    - Situations requiring identity or address verification, EDD, or the development of a comprehensive risk profile.
- Furnish updated KYC information to the CKYCR within seven days, or within any revised timeframe as notified by the Central Government.

17.0 Adoption of New Technologies

Prior to the deployment of any new technologies, products, or services, AuroPay will undertake the following actions:

- Conduct a comprehensive risk assessment to identify and evaluate potential money laundering and terrorist financing (ML/TF) risks associated with the proposed innovations.
- Implement a risk-based mitigation strategy to address identified risks, which will include the application of EDD measures and the enhancement of transaction monitoring systems, as deemed appropriate.

AuroPay will integrate these practices into its broader compliance and risk management framework to ensure that technological advancements align with regulatory expectations and internal governance standards.

18.0 GENERAL

The Company will ensure that the provisions of the applicable Acts and the Rules framed thereunder are adhered to strictly.

Where the Company is unable to apply appropriate KYC measures, the Company will close such an account or terminate the business relationship after issuing due notice to the Merchant explaining the reasons for taking such a decision. Such decisions need to be taken at a reasonably senior level. The Company will abide by all guidelines, directives, instructions, and advice of RBI and will be in force

sometimes. This document's contents shall be read with these guidelines, directives, instructions, and advice.

APPENDIX I – ENTITY WISE KYC DOCUMENT CHECKS

Particulars	Specific Checks
INDIVIDUAL CHECKS	
PAN Card / Form 60	• PAN Number is validated by third-party • Requested for Ultimate Beneficial Owner (UBO); Authorised Signatory; Power of Attorney holder; Authorisation holder
Officially Valid Document (OVD): (Any 1) Passport, driving license, proof of possession of Aadhaar number, the Voter's Identity Card, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register.	• Aadhaar Card is authenticated • Required for Ultimate Beneficial Owner (UBO); Authorised Signatory; Power of Attorney holder; Authorisation holder • Match OVD details with that on PAN (e.g.: name, birthdate, image, etc.)
Individual Address proofs (if required): Utility bills, Property/Municipal Tax receipts, Pension orders, and Letter of allotment. **Proof of address of foreign nationals:** Any document issued by the Government departments of foreign jurisdictions and/or letter issued by the Foreign Embassy or Mission in India.	• Match name and address with PAN and other documents • Match address proof with details provided during initial sign-up
Cancelled Cheque	• Bank Account details are verified
LEGAL ENTITY CHECKS	
Public/Private Limited Company • Certificate of Incorporation • Memorandum of Association (MoA) and Articles of Association (AoA) • PAN Card • Board Resolution • Ownership Structure and UBO declaration • OVD of Authorised signatory • Cancelled Cheque	• Verify name, CIN/DIN/LLP via Ministry of Corporate Affairs (MCA) Portal • Board Resolution is verified by matching authorised signatory details on AoA, MoA • OVD of Authorised signatory is verified • PAN Number of the Company is verified • Bank Account details are verified
Partnership/Limited Liability Partnerships (LLP) • Registration Certificate • PAN • Partnership Deed/LLP agreement • Power of Attorney • OVD of Authorised signatory • Cancelled Cheque	• Registration checks based on available databases • OVD of Authorised signatory is verified • PAN Number is verified • Bank Account details are verified

Sole Proprietorship • PAN and OVD of proprietor • Any two of the below documents as proof of Business: • Certificate/licence issued under the Shop and Establishment Act. • Registration Certificate • Sales and income tax returns. • VAT/ GST certificate	• OVD of Authorised signatory is verified • PAN Number is validated by third-party • Registration checks based on available databases • Bank Account details are verified

(provisional/final). • Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities. • IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT 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 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. • Cancelled Cheque	
Trusts • Registration Certificate • PAN Card • Trust Deed • Power of Attorney • OVD of Authorised signatory • list of beneficiaries, settlors, and trustees • Cancelled Cheque	• Registration checks based on available databases • OVD of Authorised signatory is verified • PAN Number is verified • Bank Account details are verified
Unincorporated Association or a body of individuals • PAN Card • Power of Attorney • Resolution of the managing body • OVD • Cancelled Cheque	• OVD of Authorised signatory is verified • PAN Number is verified • Registration checks based on available databases • Bank Account details are verified

Hindu Undivided Family (HUF) • PAN Card • Resolution of managing body • Power of Attorney • HUF Deed (if applicable) • Cancelled Cheque	• PAN Number is verified • Registration checks based on available databases • Bank Account details are verified

APPENDIX II – RESTRICTED MERCHANT CATEGORY

A Merchant shall not use Aurionpro Payments services to accept payments connected with the following businesses and business activities:

- Virtual currency, other cryptocurrencies, and tokens (that can be monetized, resold, converted, traded into physical/digital goods & services outside the virtual world)
- Prevented Drugs, prevented Drug equipment & Drug test prevention aids, Narcotics or Steroids
- Illegal substances and products
- Miracle Cures
- Forex & Currencies, Stamps, and coins
- Items or Downloads that infringe or violate Copyright, Trademark, right of publicity or privacy or any other proprietary right under the laws of any jurisdiction
- Human remains and body parts
- Firearms, weapons, or Ammunitions
- Counterfeit products and Replica Goods
- Unauthorized copyright media and software
- Merchants involved with bestiality, rape, hate, violence, or incest
- Child abuse imagery and child pornography
- Hacking and cracking materials
- Fake credentials, fake academic papers, etc.
- Gambling, gaming and/or any other activity with an entry fee and a prize, including, but not limited to casino games, sports betting, horse racing, lottery tickets, other ventures that facilitate gambling, games of skill (whether it is legally defined as a lottery) and sweepstakes.
- Stolen goods including digital and virtual goods
- Tobacco, e-cigarettes, and Alcohols
- Fireworks & Hazardous materials
- Medical consultation

- Immigration/Visa passport
- Cyber lockers
- Files sharing and storage
- Associated with purchases of annuities or lottery contracts, lay-away systems, off-shore banking or transactions to finance or refinance debts funded by a credit card
- Escort Services, Adult Contents & entertainment, Pornographies & Sexually Oriented Materials or Services
- Pyramid or Ponzi Schemes, Matrix Programs and other "Get Rich Quick" Schemes and Investment Schemes
- Ticket brokers
- Gold bars and precious metals/materials
- Extended warranties
- Telemarketing companies solicit orders primarily with outbound telephone calls, facsimile, or email. Includes "Up-Sellers."
- 3rd party/aggregation
- Collection agencies
- Payday lenders
- Credit repair companies
- Loan modification
- Government loans
- Items that promote hate, racism, religious persecution, and offensive content
- Items encouraging illegal activity
- Associated with the sale of traveler's Cheque or money orders
- Provide certain credit repair or debt settlement services, credit transactions, or insurance activities
- Companies primarily engaged in the sale of coupons, certificates, prepaid, gift cards and stored value cards
- Any activities restricted or prohibited under the applicable laws, rules, regulations, notifications, or guidelines issued by the government or the regulatory authority within the jurisdiction.

If you are not sure whether your business falls into the Restricted Business category, feel free to contact us. Our team will consider every aspect of your company to make the right decision.

Note: AuroPay and our payment processing partners reserve the right to amend, change, or add to the above listed underwriting tiers and underwriting terms and conditions at any time without notice. Our payment processing partners within their sole discretion reserve the right to decline any application at any time for any reason.