

PayBitoPro

Ongoing Monitoring Policy

(Rest of the World)



Created by:	Avishek Banerjee
Approved by:	Soumendu Roy
Documentation Version:	4.6
Submission Date:	15th Jan, 2025

CONTENTS

● <i>Introduction</i>	4
● <i>Policy Objectives</i>	4
● <i>Scope</i>	5
● <i>Ongoing Customer Due Diligence</i>	5
● Name Screening and Sanctions Monitoring	6
● Transaction and Behavioral Monitoring	7
● Dormant Account Monitoring	7
● Staff Training and Awareness	8
● Roles and Responsibilities	8
● Recordkeeping and Auditability	9
● Escalation and Reporting	9
● Governance and Review	10

1. Introduction

The purpose of this Ongoing Monitoring Policy is to define PayBitoPro's approach to continual customer and employee oversight in line with regulatory requirements, FATF Recommendations, and relevant industry guidance.

Ongoing monitoring is a core component of the firm's Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and customer protection framework. It ensures that customer behavior aligns with expected activity, staff remain compliant with regulatory standards, and risks are appropriately identified and mitigated.

2. Policy Objectives

- a.* To ensure that customer activity remains consistent with their profile and declared purpose.
- b.* To detect and address suspicious or unusual transactions in a timely and effective manner.
- c.* To maintain current and accurate customer due diligence (CDD) data.
- d.* To conduct regular employee training, including AML, complaints handling, and vulnerable customer awareness.
- e.* To ensure sanctions compliance and name screening is continuous.
- f.* To monitor dormant and high-risk accounts with enhanced scrutiny.
- g.* To provide auditable evidence of compliance to regulators and auditors.

3. Scope

This policy applies to:

- a.* All customers and counterparties engaging with PayBitoPro services.
- b.* All employees across customer-facing and compliance roles.
- c.* All business activities including cryptocurrency trading, staking, and wallet services.

4. Ongoing Customer Due Diligence (CDD)

PayBitoPro maintains a risk-based approach to monitoring CDD compliance. This includes:

- a.* Periodic Reviews of all customer records, based on their risk classification:
 - i.* **High-risk customers:** Annual KYC refresh
 - ii.* **Medium-risk customers:** Biennial KYC refresh
 - iii.* **Low-risk customers:** Triennial KYC refresh
- b.* Trigger-Based Reviews initiated by:
 - i.* Unusual or significant transactions
 - ii.* Reactivation of dormant accounts
 - iii.* Change in beneficial ownership
 - iv.* Regulatory updates or sanctions matches
 - v.* Customer profile changes (occupation, address, source of funds)



KYC documentation is reverified, and new due diligence is undertaken as required. Failure to comply with refresh requests may result in account suspension or offboarding.

5. Name Screening and Sanctions Monitoring

To comply with global sanctions regimes and PEP screening requirements:

- a.* Customers are screened at onboarding and continuously using tools such as ComplyAdvantage.
- b.* Screening includes checks against lists from OFAC, HMT, FATF, UN, EU, and Interpol.
- c.* Any positive matches trigger enhanced due diligence and immediate escalation to the MLRO.
- d.* Sanctions and PEP checks are repeated at every periodic KYC review and upon any alerts.

6. Transaction and Behavioral Monitoring

- a.* **A multi-tier transaction monitoring system is in place that includes:**
 - i.* Real-time and post-transaction alerting
 - ii.* Monitoring based on customer risk level and product usage
 - iii.* Red flag indicators for transaction types, IP location inconsistencies, counterparty risk, and volume anomalies
 - iv.* Specific attention to spot, futures, staking, and cross-chain transactions



Customers are categorized into monitoring levels (A–C) based on risk attributes like PEP status, adverse media, or industry involvement.

***b.* Watchlist Monitoring:**

- i.* **Level A:** Weekly review
- ii.* **Level B:** Monthly review
- iii.* **Level C:** Quarterly review

7. Dormant Account Monitoring

Accounts are considered dormant after 12 months of inactivity. Upon attempted reactivation:

- a.* A full KYC review is triggered.
- b.* All previously submitted documents are revalidated.
- c.* Transactional and behavioral history is reviewed.
- d.* If suspicious activity is detected, the account is escalated for further investigation and potentially reported via a SAR.

8. Staff Training and Awareness

Training ensures employees understand their responsibilities regarding monitoring, reporting, and customer care. This includes:



- a.* Initial AML/CTF training upon hire
- b.* Mandatory KYC refresher training every 6 months
- c.* Specialist sessions for compliance and customer support staff
- d.* Training on handling vulnerable customers and complaints, aligned with relevant guidance

Completion rates are tracked, and training is assessed via pre- and post-session testing. The MLRO reviews training efficacy annually and updates content as necessary.

9. Roles and Responsibilities

- a. MLRO:* Oversees all monitoring activities, investigates alerts, files SARs, and reports to regulators.
- b. Compliance Team:* Conducts periodic CDD reviews, sanctions screening, and internal audits.
- c. Investigators:* Review transaction alerts and escalations.
- d. Cybersecurity Team:* Maintains surveillance tools and analytics infrastructure.
- e. All Employees:* Required to report suspicious activity and cooperate with investigations.

10. Recordkeeping and Auditability

PayBitoPro retains:

- a.* All customer due diligence and transaction monitoring records for five years after account closure.



- b.* Staff training records for three years.
- c.* Monitoring reports, audit trails, and compliance logs for regulatory inspection.

11. Escalation and Reporting

- a.* The activity is escalated to the MLRO for review.
- b.* If deemed reportable, a Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR) is filed with the appropriate authority within two working days.
- c.* Staff are reminded that tipping-off is a criminal offense and all escalations are handled confidentially.

12. Governance and Review

This policy is reviewed annually by the MLRO or more frequently in response to:

- a.* Significant changes in regulations
- b.* Internal audit findings
- c.* Emerging threats or typologies in financial crime