XPTP

INTERNAL RULES OF PROCEDURE FOR PREVENTION OF
MONEY LAUNDERING AND TERRORIST FINANCING

(AML AND KYC POLICY)

Last Updated: April 15, 2026

1. General Provisions

1.1 XPTP ("the Service"), operated in accordance with the laws of Saint Vincent and the Grenadines, is committed to the highest standards of Anti-Money Laundering (AML) compliance and Counter-Terrorist Financing (CTF). The Service requires its operators and relevant personnel to adhere to these standards and actively prevents any actions that aim to facilitate the process of legalizing illegally obtained funds.

1.2 The Service operates as a **non-custodial cryptocurrency payment detection and forwarding service**. The Service does not hold, store, or maintain custody of user funds. Cryptocurrency transfers are detected on public blockchain networks and automatically forwarded to merchant-designated wallet addresses. Funds are held momentarily for transaction verification before automatic disbursement.

1.3 The Service does not handle, convert, transmit, or store fiat currency in any form. All transactions are conducted exclusively in cryptocurrency on public blockchain networks.

1.4 These internal rules of procedure ("Policy") establish security measures for conducting due diligence, detecting suspicious activity, and maintaining compliance across all areas of the Service's operations.

2. Definitions

2.1 Money Laundering

The conversion, transfer, acquisition, possession, or use of property derived from criminal activity, or the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of such property, knowing that the property is derived from criminal activity.

2.2 Terrorist Financing

The allocation or raising of funds to plan or perform acts of terrorism, or to finance operations of terrorist organizations, or with knowledge that the funds will be used for such purposes.

2.3 Sanctioned Person or Entity

Any individual, organization, or wallet address that appears on sanctions lists maintained by the United States Office of Foreign Assets Control (OFAC), the European Union, the United Nations Security

Council, or other relevant sanctioning bodies.

2.4 Politically Exposed Person (PEP)

A natural person who performs or has performed prominent public functions, as well as their family members and known close associates. Persons who have not performed prominent public functions for at least one year shall not be considered PEPs.

2.5 Compliance Officer

The designated person responsible for the implementation and enforcement of this Policy, transaction monitoring, and reporting of suspicious activity.

2.6 Merchant

A legal entity or individual who integrates the Service's API to accept cryptocurrency payments and to whom funds are forwarded after transaction confirmation.

2.7 Payer

An individual or entity that sends cryptocurrency through the Service's payment flow to fulfill a payment created by a Merchant.

3. Service Architecture and Compliance Implications

3.1 The Service is designed as non-custodial infrastructure. The compliance implications of this architecture are:

- **No user accounts:** The Service does not maintain user accounts, balances, login credentials, or persistent user identities.
- **No fiat interaction:** The Service operates exclusively with cryptocurrency. No fiat currency is accepted, stored, converted, or transmitted.
- **Automatic forwarding:** Upon confirmation of an incoming transfer on the relevant blockchain network, funds are automatically routed to the Merchant's designated wallet address minus the applicable service fee.
- **7-day data retention:** All payment data, transaction records, and associated metadata are automatically and permanently deleted after 7 days.
- **No personal data collection:** The Service does not collect names, email addresses, IP addresses, government identification numbers, or other personally identifiable information from Payers.

3.2 Despite the non-custodial nature of the Service, the Service maintains this AML/KYC Policy as a demonstration of good faith compliance and commitment to preventing the use of the Service for illicit purposes.

4. Customer Identification and Verification

4.1 The Service reserves the right to identify and verify any Merchant or user of the Service, regardless of transaction size or frequency.

Individual Merchants

4.2 When the Service exercises its right to verify an individual Merchant, the following information may be requested:

Information	Purpose
Full legal name	Identity verification
Date of birth	Identity verification, age confirmation
Country of residence	Jurisdiction assessment, sanctions screening
Email address	Communication, account correspondence
Cryptocurrency wallet address(es)	Transaction monitoring, sanctions screening

4.3 The Service has the right to verify the Merchant's identity based on:

- A high-resolution copy of a government-issued identity document (passport, national ID card, or driving license) showing the holder's full name, photograph, date of birth, and signature;
- Proof of residence (utility bill, bank statement, or tax document not older than three months).

Business Merchants

4.4 When the Service exercises its right to verify a business Merchant, the following documentation may be requested:

Information	Purpose
Legal entity name	Identity verification
Registration number and jurisdiction	Entity verification
Registered address	Jurisdiction assessment
Names of directors and beneficial owners	UBO identification, PEP screening
Certificate of incorporation or equivalent	Entity verification

4.5 The Service must identify the ultimate beneficial owners (UBOs) of any business Merchant subject to enhanced due diligence, defined as natural persons owning or controlling more than 25% of the entity.

5. Enhanced Due Diligence

5.1 Enhanced due diligence measures shall be applied when:

- A Merchant or associated wallet address is identified as high-risk;
- A transaction involves a wallet address with known connections to illicit activity;
- A Merchant or associated person is identified as a PEP;
- Unusual transaction patterns are detected through automated monitoring;
- The Compliance Officer determines additional scrutiny is warranted.

5.2 Enhanced due diligence may include requesting additional identification documents, source of funds documentation, detailed business description, or any other information deemed necessary by the Compliance Officer.

6. Wallet Address Screening

6.1 The Service screens all wallet addresses against:

- **OFAC Specially Designated Nationals (SDN) list** — maintained by the U.S. Department of the Treasury;
- **AMLBot risk assessment platform** — automated screening for connections to known illicit activity including mixers, darknet marketplaces, fraud, stolen funds, ransomware, and sanctioned entities;
- **Additional sanctions lists** as maintained by the European Union, United Nations, and other relevant bodies.

6.2 Screening occurs at the following points in the payment lifecycle:

- **Payment creation:** Merchant payout addresses are screened before the payment is accepted;
- **Payment detection:** Sender (payer) addresses are screened when a transfer is detected on-chain;
- **Periodic refresh:** Sanctions lists are updated daily from authoritative sources.

6.3 Transactions involving addresses identified on sanctions lists or flagged as high-risk by AMLBot shall be automatically rejected. The Service reserves the right to refuse service to any address or party that appears on applicable sanctions or risk lists without prior notice.

7. International Sanctions

7.1 The Service maintains and enforces sanctions compliance by screening against publicly available sanctions lists and commercial risk assessment tools.

7.2 The Service shall not knowingly process transactions involving:

- Individuals or entities on the OFAC SDN list;
- Individuals or entities subject to EU, UN, or other international sanctions;

- Wallet addresses associated with sanctioned persons or entities;
- Jurisdictions subject to comprehensive sanctions programs.

8. Risk-Based Approach

8.1 The Service applies a risk-based approach to compliance, in accordance with FATF recommendations. Investigative and due diligence efforts shall be proportional to the assessed risk level of each case.

8.2 Risk categories:

Category	Criteria	Measures
LOW RISK	Small transaction amounts; wallet addresses with clean history; Merchants with established track record on the Service	Standard automated screening; no additional verification required
NORMAL RISK	No specific risk indicators; standard transaction patterns; Merchant cannot provide complete documentation but has no negative indicators	Standard automated screening; periodic review
HIGH RISK	PEP or PEP associate; negative media coverage; wallet address with connections to illicit activity; unusual transaction patterns; high-risk jurisdiction	Enhanced due diligence; manual review by Compliance Officer; possible suspension of service

8.3 The Service's policy is to operate with low and normal risk Merchants. Merchants assessed as high risk may be subject to enhanced verification requirements or service termination.

9. Transaction Monitoring

9.1 The Service employs automated transaction monitoring through blockchain analysis and third-party risk assessment tools (including AMLBot) to detect:

- Transactions involving sanctioned wallet addresses;
- Transactions involving addresses connected to known illicit activity;
- Unusual transaction patterns or volumes;
- Structuring or layering attempts.

9.2 Transaction monitoring cases may be initiated automatically by the screening system or manually by the Compliance Officer.

9.3 The Compliance Officer shall review flagged transactions and determine appropriate action, which may include enhanced due diligence, transaction rejection, or service termination.

10. Geographic Restrictions

10.1 The Service shall not knowingly provide services to:

- Citizens, residents, or persons located within the United States of America, its territories, or possessions;
- Citizens, residents, or persons located within jurisdictions subject to comprehensive sanctions by OFAC, the United Nations, or the European Union, including but not limited to: Iran, North Korea, Cuba, Syria, Russia, Belarus, the Crimea region, Myanmar, Venezuela, Zimbabwe, Sudan, and South Sudan;
- Any person or entity appearing on applicable sanctions lists.

10.2 The Service reserves the right to terminate service to any user reasonably believed to be in violation of these geographic restrictions.

11. Prohibited Activities

11.1 The Service shall not be used for:

- Money laundering or terrorist financing;
- Sanctions evasion;
- Fraud, deception, or misrepresentation;
- Ransomware or extortion payments;
- Darknet marketplace transactions;
- Sale of controlled substances, arms, or prohibited goods;
- Child exploitation material;
- Ponzi schemes, pyramid schemes, or similar fraudulent operations;
- Violation of export controls;
- Any activity illegal under applicable law.

11.2 The Service reserves the right to refuse, suspend, or terminate service and report suspicious activity to relevant authorities.

12. Data Collection and Record-Keeping

12.1 In accordance with the Service's privacy-first architecture, all payment data is automatically and permanently deleted after 7 days. This includes transaction records, wallet addresses, webhook logs, and associated metadata.

12.2 Where enhanced due diligence has been conducted and verification documents have been collected, such documents shall be retained for the duration required by applicable law or for a minimum

period as determined by the Compliance Officer, separate from the standard 7-day payment data retention.

12.3 Aggregated, anonymized metrics (transaction counts and volume totals) are maintained for operational purposes. These metrics contain no information that can be linked to individual users or transactions after the 7-day retention window.

13. Reporting

13.1 The Compliance Officer is responsible for identifying and reporting suspicious transactions in accordance with applicable law.

13.2 Where the Compliance Officer determines that a transaction or pattern of transactions is suspicious, a Suspicious Transaction Report (STR) may be filed with the relevant Financial Intelligence Unit (FIU) or Financial Monitoring Service (FMS).

13.3 All relevant personnel are prohibited from informing Merchants or Payers that their activity has been flagged as suspicious or that a report has been or may be filed (tipping-off prohibition).

14. Compliance Officer

14.1 The Service shall designate a Compliance Officer responsible for:

- Implementation and enforcement of this Policy;
- Monitoring transactions and reviewing flagged activity;
- Conducting or supervising enhanced due diligence;
- Filing suspicious transaction reports;
- Ensuring sanctions list updates are applied;
- Training relevant personnel on AML/CTF obligations;
- Periodic review and updating of this Policy.

15. Training

15.1 All relevant personnel shall receive training on AML/CTF obligations, recognition of suspicious activity, and the procedures outlined in this Policy.

15.2 Training shall be conducted upon onboarding and updated at least annually, or more frequently as warranted by changes in regulation or this Policy.

16. Policy Review

16.1 This Policy shall be reviewed and updated at least annually, or more frequently as required by changes in applicable law, regulation, industry standards, or the Service's operations.

16.2 Material changes to this Policy will be documented and communicated to all relevant personnel.
