

CRYPTO PAYMENTS POLICY

Atlas Tech Solutions B.V. / pro1bet.com

Version: 1.1

Effective Date: 20.11.2025

Approved By: Executive Management

Policy Owner: AML Compliance Officer (AMLCO)

1. General policies

1.1 Purpose

This policy defines how the Company processes cryptocurrency deposits and withdrawals via **GammaG**, ensuring AML/CTF compliance, player protection, and adherence to Curaçao GCA licensing requirements.

1.2 Scope

Applies to:

- All players using cryptocurrency.
- All employees handling payments, compliance, fintech operations, and fraud monitoring.
- All Company wallets and infrastructure connected to GammaG.

1.3 Accepted Cryptocurrencies

The Company accepts cryptocurrencies supported by **GammaG**, including (but not limited to):

- Bitcoin (BTC)
- Ethereum (ETH)
- Tether (USDT)
- USD Coin (USDC)
- Litecoin (LTC)
- Tron (TRX)
- Additional assets approved by the Compliance Department.

The Company may suspend or remove assets at any time based on risk or regulatory requirement.

1.4 Deposit Process

- A unique wallet address is generated per transaction through GammaG.
- Deposits are credited after receiving the required blockchain confirmations.
- Player is responsible for network (gas) fees.
- Deposits are automatically converted to the Company's treasury currency (EUR/USD) or retained as crypto depending on treasury settings.
- Deposits from third parties, mixers, or unknown sources are prohibited.

1.5 Withdrawal Process

- Withdrawals are processed **only after KYC verification**.
- Wallet addresses must belong to the verified player and pass blockchain risk screening via GammaG's monitoring tools.
- High-risk addresses cannot be used and require Enhanced Due Diligence.
- Withdrawal fees are deducted from the withdrawal amount unless otherwise stated.

1.6.Exchange Rate Policy

- The exchange rate applied is the rate at the moment GammaG confirms the blockchain transaction.
- The Company is not responsible for crypto volatility or price changes occurring before confirmation.

1.7 Transaction Monitoring

The Company uses:

- GammaG risk analysis engine
- Blockchain analytics tools
- Internal AML rules
- Curaçao GCA risk-based thresholds

High-risk cryptocurrency flows undergo EDD or are blocked.

1.8 Prohibited Activities

- Payments via coin tumblers/mixers
- Privacy coins (if not explicitly allowed by Compliance)
- Funds from darknet or sanctioned entities
- Third-party transfers
- Wallet addresses linked to illegal activity

1.9 Record Keeping

All crypto transaction logs, risk assessments, KYC documents, and analytics results are stored **at least 5 years** as required by the GCA AML Framework.

2- CRYPTO RISK ASSESSMENT FRAMEWORK

2.1 Risk Categories

- **Country Risk** (player location, FATF lists)
- **Wallet Risk** (sanctions exposure, mixers, darknet)
- **Transaction Behaviour Risk** (volume, pacing, pattern)
- **Source of Funds Risk**
- **Game Play Behaviour Risk** (fraud indicators)

Each transaction is scored low/medium/high risk.

Mitigation Measures

- Automatic blocking of high-risk wallet categories
- Mandatory EDD for medium/high-risk customers
- Withdrawal delay for suspicious behaviour
- Real-time monitoring via GammaG tools

2.2. WALLET VERIFICATION SOP

(Standard Operating Procedure)

Step 1 — Player submits a withdrawal request

The system checks:

- KYC status
- Account behavior
- Wallet risk score through GammaG

Step 2 — Ownership Verification

For medium/high-risk:

- Signed message from wallet
- Screenshot of wallet interface with date
- Video of logged-in wallet

Step 3 — Blockchain Tracing

Compliance reviews:

- Past transactions
- Risk flags
- Interaction with mixers or sanctioned addresses

Step 4 — Decision

- Approve
- Reject & return funds
- Hold for additional documents
- Report suspicious transactions

2.3. PLAYER-FACING T&Cs — CRYPTO SECTION

Crypto Payments

1. Cryptocurrency payments are processed through **GammaG**, the Company's authorized crypto payment processor.
2. Each deposit must be sent to the unique address generated for the transaction.
3. Deposits are credited after the required blockchain confirmations.
4. The Company is not responsible for incorrect addresses, transaction delays, or blockchain fees.
5. Withdrawals are sent only to wallets owned and verified by the player.
6. The Company may request additional documents before processing withdrawals.
7. Third-party payments and mixers are forbidden and result in account suspension.
8. The Company determines the exchange rate based on GammaG's confirmed rate at the time of transaction.

2.4. INTERNAL COMPLIANCE STRUCTURE

Compliance Officer

- Ensures AML/CTF compliance
- Audits crypto transactions
- Approves/denies high-risk withdrawals
- Files UTRs to FIU Curaçao
- Reports compliance metrics to GCA

Crypto Risk Analyst

- Monitors GammaG analytics
- Reviews wallet behavior
- Flags suspicious patterns

Support Staff

- Assists players with verification
- Reports unusual activity to Compliance

2.5 RECORD-KEEPING & AUDIT REQUIREMENTS

Retention Period: 5 Years Must store:

- Crypto transaction logs
- KYC/EDD documents
- Risk scoring reports
- Communication with players
- Audit logs from GammaG

Audit Readiness

The Company must ensure:

- Transaction history is exportable
- Player data is structured
- AML cases are documented

- Risk assessments are up to date

2.6. SUSPICIOUS ACTIVITY RED FLAGS

- Deposits from high-risk exchanges or darknet markets
- Multiple unrelated wallet addresses
- Instant deposit + withdrawal behaviour
- Structuring to avoid thresholds
- Use of privacy-enhanced transactions
- High-risk IP/geolocation

Approved by:

Executive Corporate Management

Andrii Iudintsev

Managing Director

A handwritten signature in dark ink, appearing to read 'Andrii Iudintsev', with a large, stylized flourish at the end.