AlgoHive
Where Smart Capital Gathers

Anti-money laundering (AML) and Counter-Terrorist Financing (CTF)

We require all Algohive customers to comply with the Financial Intelligence Center Act (FICA) in order for us to maintain strict Know Your Customer (KYC) and AML standards. The process is different for individuals and businesses. We have appointed a third-party service provider, Didit.me to ensure that we comply with FICA through automatic sanctions screening and risk rating. On signing up for a Algohive account you are able to immediately transact on our platform. In order for you to transact and withdraw or deposit FIAT in your account you will need to be fully verified.

Key components of our AML and CTF framework include the following:

- We have appointed an internal Compliance Officer. This person is responsible for oversight of compliance with the relevant legislation, regulations, rules and industry guidance;
- We have a risk-based approach to the assessment and management of money laundering and terrorist financing risks;
- When opening a Algohive account, to ensure we meet KYC standards, our customers are required to provide certain personal details and documentation. Algohive may perform enhanced due diligence procedures for customers presenting a higher risk, such as those transacting in large volumes;
- We monitor customer activity on our platform on an ongoing basis and maintain risk-based systems and procedures for this;
- We have internal procedures in place for reporting suspicious activity;
- All relevant employees of Algohive receive a framework and guidance on raising awareness on suspicious activity;
- We keep and maintain appropriate KYC records for the minimum prescribed periods and update as necessary;

KYC

Each participant having an account with Algohive has to go through a KYC process. Algohive's approach to KYC is a typical 4-eye approach as follows:

Creation of account:

- The participant is required to enter a mobile number and PIN on account creation (signup)
- The mobile number gets approved through a 3rd party NI-USSD system or through our APP linked to their device.
- The identity is created with limited functionality until all documents are verified.

Verification of participant:

- The participant is required to enter his/her ID number and address
- The participant receives a request to upload copy of ID and proof of address

- The participant is required to provide 3-month's bank statement as "proof of funds"
- The 3rd party service provided by Didit.me
  - that the ID number is valid
  - ID document is valid
  - proof of address is valid and within a 3-month period from current date

If all conditions above are valid, the request to verify the identity is approved.

- Algohive receives the approved or rejected application from Didit.me
- If the application is approved by 3rd Party: Algohive reviews the documentation provided by participant: double checks the validity of the documents and actions the final approval of the application
- The participant now has access to all the actions on the platform and is able to transact, send and receive FIAT currency.
- Participants will need to enter and provide proof of their bank account details in order to withdraw funds.

Declaration

Each participant having an account with Algohive has agreed to the terms and conditions. Additionally, for South Africans, we have a mandate that is signed on the first deposit each year to approve Algohive as a reportable institution that affects your foreign capital allowance to the SARB/SARS.

Upon each deposit and withdrawal, a client will be notified that their allowance used has been influenced and that they can log in to their account profile to see the current state of allowances used.

Further information on regulatory reportable transactions will be displayed. These are transactions that externalise crypto to other exchanges.

Reporting

Reporting of each participant's transactions can be done and grouped by a selected time period (hour, day, week, month and/or year): The following information to be reported on:

- All exchanges (FIAT ↔ Crypto)
- Send and Receive (FIAT & Crypto)

Currently, Algohive monitors transactions via our business intelligence tools, which include:
- approval of each fiat deposit and withdrawal
- high value transactions
- the velocity of transactions
- the volume of transactions

Algohive blocks accounts if suspicious behaviour is detected. The blocked participant will be unable to withdraw, trade or send until further investigation is complete.

Additional Reporting

- The participant's foreign allowance used is calculated and limits placed on client accounts.
- Additionally, information held, monitors and customizes limits on participant functionality, such as:
  - Tax Number
  - SDA - Single Discretionary Allowance
  - FIA – Foreign Investment Allowance - PIN Entry
  - Declaration of funds in
  - Non- Reportable - Value of transfers

Exchange Control Limits

Algohive automatically places limits based on your foreign allowances. These allowances are geared towards the Exchange control regulations and will limit each user to stay within these limits. An example is that South African consumers may only externalise R1m per calendar year through a Single Discretionary Allowance. Additional allowance may be applied for through SARS.

AlgoHive
Where Smart Capital Gathers

Account Lock

Suspicious account activity results in a lock by Super admin. This account lock places entire account functionality under lockdown, including all API's.

Beneficiary Creation

No consumer can send funds internally or externally without the creation of a beneficiary.

These beneficiaries get checked on creation:
- Bank Account - Bank Verification Check

Sanction Checks

Algohive checks high risk clients against our 3rd party partner Didit.me. They provide us updates if a customer appears on the sanction database periodically. If a client appears on the list, the account is placed in lock whilst further investigation ensues.