



AML / CFT Policy

Version: January 2026



CONTENTS

1.	INTRODUCTION	3
2.	LEGAL FRAMEWORK	3
3.	SCOPE	3
4.	GOVERNANCE	3
5.	RISK-BASED APPROACH AND CLIENT ACCEPTANCE	4
6.	CUSTOMER DUE DILIGENCE	4
7.	SANCTIONS COMPLIANCE	5
8.	CRYPTO-ASSET-SPECIFIC CONTROLS	5
9.	TRANSACTION MONITORING AND REPORTING	5
10.	RECORD KEEPING	6
11.	TRAINING AND AWARENESS	6
12.	WHAT WE ASK OF OUR CLIENTS	6
13.	REVIEW OF THIS POLICY	6
14.	CONTACT US.....	6



1. INTRODUCTION

1.1. NAGA X Ltd ("NAGA X" or the "Company") is a company registered in Cyprus under number HE 424746 and authorised by the Cyprus Securities and Exchange Commission ("CySEC") as a Crypto-Asset Service Provider ("CASP") under Regulation (EU) 2023/1114 on markets in crypto-assets ("MiCA"), CASP registration number 009/23. Its registered office is at Agias Zonis 11, 3027 Limassol, Cyprus.

1.2. The Company is committed to preventing its services from being used for money laundering, terrorist financing or the evasion of financial sanctions. This Policy summarises, for clients and the public, the measures the Company applies. It does not form a complete description of the Company's internal procedures.

2. LEGAL FRAMEWORK

2.1. The Company's AML/CFT framework is designed to comply with, in particular:

- the Prevention and Suppression of Money Laundering and Terrorist Financing Law of 2007 (Law 188(I)/2007), as amended;
- CySEC's Directive for the Prevention and Suppression of Money Laundering and Terrorist Financing, and related CySEC circulars;
- Regulation (EU) 2023/1114 (MiCA);
- Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets (the "Transfer of Funds Regulation" or "Travel Rule");
- the Law on the Establishment of the National Sanctions Implementation Unit and the Implementation of Restrictive Measures and National Sanctions of 2025 (Law 150(I)/2025);
- EU restrictive measures and UN Security Council sanctions; and
- relevant guidance of the European Banking Authority, the Financial Action Task Force ("FATF") and MONEYVAL, and the findings of the Cyprus National Risk Assessment on virtual assets.

3. SCOPE

3.1. This Policy applies to all crypto-asset services the Company provides: custody and administration of crypto-assets; exchange of crypto-assets for funds and for other crypto-assets; execution of orders and reception and transmission of orders; transfer services; and portfolio management (non-discretionary copy trading).

3.2. It applies to all clients, whether retail or professional, to all employees, directors and outsourced staff, and, to the extent relevant, to the Company's service providers.

4. GOVERNANCE

4.1. Board of Directors. The Board has adopted an internal Anti-Money Laundering and Terrorist Financing Manual and approves all changes to it. The Board sets the Company's AML/CFT policy principles, ensures adequate resources and systems, and reviews and approves the annual report of the Anti-Money Laundering Compliance Officer. In line with Article 58D of Law 188(I)/2007, a designated member of the Board is responsible for the implementation of the AML/CFT legal framework.

4.2. Anti-Money Laundering Compliance Officer ("AMLCO"). The AMLCO is a senior officer who reports directly to the Board, has access to all relevant information and is independent of business functions. The AMLCO oversees the Company's AML/CFT policies and procedures, receives and assesses internal suspicious-activity reports, decides on reports to the authorities, and prepares an annual report to the Board, which is submitted to CySEC. All employees must report any knowledge or suspicion of money laundering or terrorist financing to the AMLCO without delay.



4.3. Internal audit. The internal audit function reviews the adequacy and effectiveness of the Company's AML/CFT framework at least annually and reports its findings to the Board.

4.4. Business-wide risk assessment. The Company assesses the money laundering and terrorist financing risks it faces, taking into account its clients, the countries it operates in, its services and crypto-assets, and its delivery channels, and updates this assessment periodically and whenever there is a material change.

5. RISK-BASED APPROACH AND CLIENT ACCEPTANCE

5.1. The Company applies a risk-based approach: the higher the assessed risk, the more extensive the due diligence and monitoring. Each client is assessed at onboarding, taking into account their background, country of residence and nationality, the services requested, the expected nature and level of activity, and the expected source of funds, and is classified as low, medium or high risk. A client classified as higher risk is not downgraded afterwards.

5.2. The Company does not establish or continue a relationship with:

- persons who fail or refuse to provide the information needed to verify their identity and economic profile;
- persons under the age of 18;
- shell banks;
- persons subject to UN, EU or Cyprus sanctions or other applicable restrictive measures;
- persons resident in jurisdictions the Company has designated as restricted;
- anonymous accounts, accounts in fictitious names, or clients using anonymising technologies that prevent tracing of transactions;
- clients whose activity involves mixing or tumbling services, or privacy-enhancing crypto-assets, without sufficient transparency;
- clients whose wallets are linked to illicit activity by blockchain analytics;
- unlicensed or unsupervised gambling or betting businesses; and
- clients whose activity is inconsistent with the information held on them and cannot be explained.

5.3. The Company provides its services only to residents of the EU/EEA Member States in which it is entitled to operate. It does not accept residents of the United States of America or Canada, or of other jurisdictions it designates as restricted on its website.

6. CUSTOMER DUE DILIGENCE

6.1. Identification and verification. Before establishing a business relationship or carrying out any transaction, the Company identifies the client and verifies their identity and residential address on the basis of documents, data or information from reliable and independent sources. Where the client is a legal entity, the Company also identifies its beneficial owners and controlling persons and understands its ownership and control structure.

6.2. Purpose of the relationship. The Company obtains information on the purpose and intended nature of the business relationship, the client's occupation and expected activity, and the expected source of funds. This may include crypto-asset-specific information such as wallet addresses and evidence of their ownership.

6.3. Enhanced due diligence. The Company applies enhanced measures to higher-risk clients and situations, including clients connected with high-risk third countries identified by the FATF or the European Commission, politically exposed persons, and complex or unusual transactions. Enhanced measures may include further identification documents, evidence of source of funds and source of wealth, closer ongoing monitoring and senior management approval.



6.4. Politically exposed persons. The Company identifies whether a client, or a family member or close associate, is a politically exposed person ("PEP"). A relationship with a PEP is established only with senior management approval and is subject to enhanced ongoing monitoring.

6.5. Ongoing due diligence. The Company keeps client information up to date and reviews client risk profiles periodically according to their risk level, and whenever relevant circumstances change. Clients may be asked to provide updated documents.

7. SANCTIONS COMPLIANCE

7.1. The Company maintains a risk-based Sanctions Compliance Programme. Before onboarding and on an ongoing basis, it screens clients, their beneficial owners and connected parties against applicable sanctions lists, including those of the United Nations Security Council and the European Union, as well as PEP and adverse media sources.

7.2. Where a sanctions match is confirmed, the relevant account is restricted immediately, assets are frozen where required by law, and the matter is escalated to the AMLCO and reported to the competent authorities.

7.3. Transfers involving addresses or counterparties linked to sanctioned persons or jurisdictions are blocked.

8. CRYPTO-ASSET-SPECIFIC CONTROLS

8.1. Blockchain analytics. The Company uses blockchain analytics to trace wallets and assess the risk of incoming and outgoing transfers, including exposure to mixers or tumblers, darknet markets, sanctioned entities, fraud and other illicit sources. Transfers with unacceptable risk may be rejected, returned, suspended or escalated to the AMLCO.

8.2. Travel Rule. In accordance with Regulation (EU) 2023/1113, for every transfer of crypto-assets, regardless of amount, the Company collects, verifies, transmits and retains information on the originator and the beneficiary. For outgoing transfers this includes:

- the full name of the originator and of the beneficiary;
- the distributed ledger address or crypto-asset account number of both;
- a unique transaction identifier where no crypto-asset account is used; and
- for the originator, one of: address, national identity number, customer identification number, or date and place of birth.

This information is exchanged securely with the counterparty CASP before or at the time of the transfer and handled in line with the GDPR. For incoming transfers, the Company checks that the required information has been received and may reject, return or suspend a transfer where information is missing or incomplete.

8.3. Self-hosted wallets. For transfers to or from a self-hosted address (a wallet not held with a CASP), the Company obtains and holds the originator and beneficiary information. Where the amount exceeds EUR 1,000, the Company takes measures to verify that the address is owned or controlled by its client, and the client must cooperate with those measures.

8.4. No cash and no anonymity. The Company does not accept physical cash, does not open anonymous accounts, and does not support transactions designed to obscure the origin or destination of crypto-assets.

9. TRANSACTION MONITORING AND REPORTING

9.1. The Company monitors client transactions and activity on an ongoing basis, using automated systems and manual review, to detect unusual or suspicious activity and activity inconsistent with the client's profile.

9.2. Where the Company knows, suspects or has reasonable grounds to suspect money laundering or terrorist financing, the AMLCO reports to the Unit for Combating Money Laundering (MOKAS), the Cyprus Financial



Intelligence Unit. The Company may suspend transactions or restrict accounts while a matter is assessed, and is prohibited by law from disclosing a report to the client or third parties ("tipping off").

9.3. The Company cooperates fully with MOKAS, CySEC, law enforcement and other competent authorities in accordance with applicable law.

10. RECORD KEEPING

10.1. The Company retains customer due diligence documents and information, transaction records and supporting evidence, Travel Rule information, and relevant correspondence for at least five (5) years after the end of the business relationship or the occasional transaction, or longer where required by law or a competent authority. Records are made available to MOKAS and CySEC on request.

11. TRAINING AND AWARENESS

11.1. All employees, including outsourced staff involved in client activity, complete mandatory AML/CFT and crypto-asset risk training at least annually, delivered with a specialised external provider. The training programme is approved by the Board and updated for regulatory developments and emerging crypto-asset risks.

12. WHAT WE ASK OF OUR CLIENTS

12.1. To help the Company meet its legal obligations, clients must:

- provide accurate, complete and up-to-date information and documents when asked, including on source of funds or wealth;
- use the account only on their own behalf and only with crypto-assets and funds that belong to them;
- send and receive transfers only from and to addresses or accounts they own or are entitled to use, and cooperate with ownership checks; and
- inform the Company promptly of any change in their personal details or circumstances.

12.2. Failure to provide requested information may lead to delays, refusal of transactions, restriction of services or termination of the relationship, in line with the Client Agreement.

13. REVIEW OF THIS POLICY

13.1. The AMLCO reviews the Company's AML/CFT framework at least annually and whenever there are material changes in law, risk or the Company's services. Changes to the internal Manual are approved by the Board.

14. CONTACT US

14.1. For questions about this Policy, contact support@nagax.com . Documents requested for verification should be provided as soon as possible to avoid delays to transactions.