1. INTRODUCTION

This Anti-Money Laundering and Know Your Customer Policy (hereinafter - the "AML/KYC Policy") is designated to prevent and mitigate risks of Cryptostorm related to money laundering and associated risks. This is a short extract of key principles of the internal Policy and should not be seen as a complete document. You can request the full document by contacting customer support of the Company.

Domestic and international regulations require Cryptostorm to implement effective internal procedures and mechanisms to prevent money laundering, terrorist financing, drug and human trafficking, proliferation of weapons of mass destruction, corruption and bribery and to take action in case of any form of suspicious activity from its Customers.

AML/KYC Policy covers the following matters:

- appointing an Anti-Money Laundering Compliance Officer (AMLCO) and making sure that employees know to report any suspicious activity to him;
- identifying the responsibilities of senior managers and providing them with regular information on money laundering risks;
- training relevant employees on their anti-money laundering responsibilities;
- documenting and updating anti-money laundering policies, controls and procedures;
- introducing measures to make sure that the risk of money laundering is taken into account in the day-to-day running of your business;
- Forwarding/reporting all sustained suspicions to the relevant authority;
- Promptly responding to all communication from the relevant authority.

2. GENERAL PRINCIPLES

Before the company can execute any transaction for any new Customer, a number of procedures need to be in place and carried out:

- AML procedures, namely identification, record-keeping, discovering and monitoring unusual or suspicious transactions and as appropriate internal reporting and control;
- Employees know their responsibilities and the company's procedures;
- Relevant training is being undertaken;
- All relevant requests from outside sources are forwarded directly to the AMLCO.

3. IDENTITY VERIFICATION

Whenever the company receives supporting documents related to a new Customer's identity, it needs to be completely satisfied that they demonstrate the existence of the new Customer as a real natural or legal person and that they are indeed whom they say they are. Although the company will at times rely on third party sources as part of its fact checking procedure when onboarding Customers, the company bears ultimate legal responsibility for the checks being satisfactory.

Customer's identification information will be collected, stored, shared and protected strictly in accordance with the company's Privacy Policy and related regulations that correspond to the GDPR requirements.

4. ANTI-MONEY LAUNDERING COMPLIANCE OFFICER

AMLCO is ultimately responsible for implementing the regulations concerning AML. For the sake of ease of navigation in this document 'compliance officer' and 'AMLCO' refer to the same person; however, the specific tasks of each role are different

As noted above, the AMLCO is a person of authority with access to any and all relevant information for the completion of his duties.

You can contact our AMLCO department by emailing us at:
support@cryptostorm.net.

5. MONITORING TRANSACTIONS

The constant monitoring of the Customers' accounts and transactions is an imperative element in the effective controlling of the risk of Money Laundering and Terrorist Financing.

In this respect, the AMLCO shall be responsible for maintaining as well as developing the on-going monitoring process of the company.

6. RISK ASSESSMENT

The company shall apply appropriate measures and procedures, by adopting a risk-based approach, so as to focus its effort in those areas where the risk of Money Laundering and Terrorist Financing appears to be comparatively higher.

Further, the AMLCO shall monitor and evaluate, on an on-going basis, the effectiveness of the measures and procedures of this Policy.

The adopted risk-based approach that is followed by the company, and described in the Policy, has the following general characteristics:

- recognises that the money laundering or terrorist financing threat varies across Customers, countries, services and financial instruments;
- allows the board of directors to differentiate between Customers of the company in a way that matches the risk of their particular business;
- allows the Board to apply its own approach in the formulation of policies, procedures and controls in response to the Company's particular circumstances and characteristics;
- helps to produce a more cost-effective system;
- promotes the prioritisation of effort and actions of the company in response to the likelihood of Money Laundering and Terrorist Financing occurring through the use of the services of the company.

The risk-based approach adopted by the company, and described in the Policy, involves specific measures and procedures in assessing the most cost effective and appropriate way to identify and manage the Money Laundering and Terrorist Financing risks faced by the company.

7. SANCTIONS

The Company is prohibited from transacting with individuals, companies and countries that are under international sanctions.

8. PROHIBITED COUNTRIES

The Company does not provide services to persons residing in countries that:

- Were black-listed by international organisations due to money laundering risks;
- Consider services of the Company to be illegal and banned.

Full list of such countries is available in the full version of the Anti-Money Laundering Policy and can be accessed by requesting the same from Cryptostorm. Company reserves the right to update this list by the decision of the AMLCO having effect prior to updating of this document.