March 10, 2022

Anti-Money Laundering and Countering the Financing of Terrorism Policy

SIGTERM Inc.

I. Introduction

1. The objective of SIGTERM Inc. (SIGTERM) is to take an advantage over high volatility and accessibility of digital asset markets. SIGTERM is focusing on building automated trading system and managing digital assets. In order to achieve strong, reliable profit in highly volatile digital asset markets, SIGTERM is, instead of pursuing high-risk profits, concentrating on improving robustness of its strategy. Statistical arbitrage is one of its important strategies that finds profit in the asset price imbalances in portfolio.

2. SIGTERM is committed to the highest ethical standards regarding anti-money laundering (AML) and countering the financing of terrorism (CFT) consistent with the Republic of Korea's laws and regulations: (i) Financial Transaction Reports Act (FTRA), (ii) the Proceeds of Crime Act (POCA), and (iii) the Act on Prohibition Against the Financing of Terrorism and Proliferation of Weapons of Mass Destruction (PFOPIA). This AML/CFT Policy (the Policy) aims to safeguard SIGTERM against money laundering (ML) and the financing of terrorism (FT or TF). The Policy outlines the principles and minimum standards of internal AML/CFT controls which should be adhered to by SIGTERM to mitigate reputational, regulatory, legal and financial loss risks.

II. Scope and Applicability

3. The staff of SIGTERM, its governing bodies and every other person working for SIGTERM are required to adhere to this Policy to protect SIGTERM, and its reputation, from being misused for ML and/or TF by ensuring that they discharge their responsibilities in a manner that enables the full implementation of this Policy.

III. Principles

4. SIGTERM shall ensure that its funds are not used to finance any illegal acts related to ML or TF.

5. The Policy shall be consistent with the relevant United Nations (UN) Conventions and Recommendations of the Financial Action Task Force (FATF).

6. SIGTERM shall take steps to encourage its customers to adopt policies and procedures that are consistent with the principles set out in this Policy, with the purpose of safeguarding SIGTERM resources from being used for ML or the FT.

7. SIGTERM's customers shall be responsible for identifying and mitigating the risks of ML and TF in deploying and managing SIGTERM resources.

IV. Purpose and Objectives

8. The purpose of the Policy is to provide principles and guidance regarding AML/CFT requirements and risks and to meet the following objectives:

(a) Prevent the abuse of the SIGTERM's resources for ML and/or FT;

(b) Meet applicable legal requirements and international standards in jurisdictions where SIGTERM and its customers operate;

(c) Mitigate any reputational risk;

(d) Guard against establishing any relations or undertaking any transaction that may relate to or may facilitate ML and/or FT or any other illicit activity;

(e) Exercise due diligence when dealing with customers, persons appointed to act on behalf of customers and connected parties of the customers; and

(f) Continuously review and update its AML/CFT Policy and its corresponding AML/CFT Standard as threats and international standards evolve to prevent and detect ML and/or FT.

V. Definitions

9. For the purposes of this Policy the following terms shall have the meaning set out below:

(a) Beneficial Owner means the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

(b) Board means the Board of SIGTERM.

(c) Customer Due Diligence (CDD) refers to identifying the customer and verifying the customer's identity as well as obtaining information on the purpose and intended nature of the business relationship and identifying the Beneficial Owner for SIGTERM to guard against the dangers of ML and other financial crimes in providing products and services for customers.

(d) Financing of Terrorism (FT) or Terrorist Financing (TF) is defined as the commission of any offence as set out in Article 2 of the International Convention for the Suppression of the Financing of Terrorism.

(e) Money Laundering (ML) refers to:

(i) The conversion or transfer of property, knowing that such property is derived from crime, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of the crime to evade the legal consequences of his or her actions;

(ii) The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing such property is derived from crime; or

(iii) The acquisition, possession or use of property, knowing at the time of receipt that such property was derived from a criminal offence.

(f) Risk Based Approach (RBA) to AML/CFT is the process of identifying, assessing and understanding ML/TF risks to which SIGTERM is exposed and to take measures commensurate to those risks to mitigate them effectively.

VI. Key Provisions

10. SIGTERM shall adopt and implement a continuous RBA to identify, assess and understand its ML and TF risks. It shall also ensure measures to mitigate ML and/or TF are commensurate with the risks identified, enabling decisions on how to allocate its resources in the most effective way.

11. Under this approach, it will adhere to the following to manage AML/CFT risk:

(a) Know Your Customer (KYC)

(i) SIGTERM shall apply CDD on customers (including their Beneficial Owners) with which the SIGTERM enters a business relationship.

(ii) SIGTERM shall take reasonable measures to duly assess the purpose, economic rationale and overall AML/CFT and related integrity aspects of the customers and its Beneficial Owners to avoid being involved in relationships structured for the purposes of ML and TF.

(iii) SIGTERM will not engage with, and will terminate the existing business relationship if any, with:

1. customers who do not cooperate with its CDD efforts;
2. customers engaged in activities prohibited under the Policy; or
3. customers who are currently under any financial sanctions imposed by United Nations.

(b) Know Your Employee (KYE)

(i) As SIGTERM's funds are sourced solely from its directors/employees and it has no customers, SIGTERM shall check identification information of its existing and new executives, directors, and employees (Directors/Employees) when hiring them so as to prevent them from getting involved in ML and TF activity.

(ii) Directors/Employees are only accepted by SIGTERM only if their identifications are verified and guaranteed.

(iii) In the process of KYE measures, Directors/Employees shall submit their ID, passbook copy, resident registration certificate, credit rating, and the like. Any changes to their information should be immediately reported to SIGTERM.

(c) Ongoing Monitoring: For the purpose of preventing ML and TF, SIGTERM shall establish procedures to identify unusual transaction or patterns through a transaction monitoring system to ensure that its transactions take place without any technical errors.

(d) Reporting: Any suspicious information or red flag that comes to the knowledge of the reporting officer indicating ML/TF must be immediately reported by such reporting officer to the National Intelligence Service in Korea or the Korea Financial Intelligence Unit (KoFIU) without informing the customer or other third parties that a suspicious activity is being reported or investigated.

(e) Record Keeping: SIGTERM shall keep, for at least 5 (five) years from the completion of each business relationship, all records on KYC/KYE documents, executed transactions, reports of suspicious transactions, and the like.

(f) Confidentiality: SIGTERM will ensure the information on customers and transactions obtained while fulfilling AML/CFT requirements is kept confidential.

(g) Education and Training for Employees: SIGTERM shall develop and operate education and training programs for its employees to better enable them to follow the Policy.

(h) Review: SIGTERM shall review and examine its AML/CFT Policy and maintain an effective implementation of the AML/CFT Policy for the SIGTERM's businesses reflecting international best practices, consistent with evolving FATF Recommendations and changing requirements as well as the Republic of Korea's laws and regulations.

VII. Key Responsibilities

12. Board: The Board is responsible for ensuring governance and oversight of the SIGTERM's risk management framework and controls regarding ML and FT.

13. Internal Audit: The department independent from the AML/CFT office shall review and evaluate appropriateness and effectiveness of its AML/CFT work and to address problems with regard to the work.

14. Staff of SIGTERM, its governing bodies and every other person working for it shall be responsible for:

(a) Complying with the SIGTERM's AML/CFT Policy, standard and controls;

(b) Familiarizing themselves with and acting in accordance with relevant SIGTERM processes and procedures to manage AML/CFT compliance; and

(c) Reporting to the reporting officer without undue delay any suspicions (or actual occurrences) or red flags of ML/TF activities.

VIII. Amendment to the Policy

15. The Board shall approve the implementation of the AML/CFT Policy and any amendments thereto.

IX. Review

16. This Policy shall be reviewed at such intervals as required, to reflect international best practices, consistent with evolving FATF recommendations as well as the Republic of Korea's laws and regulations, or as otherwise required by the Board.

Supplementary Provision

This Policy shall become effective on March 10, 2022.