Anti-Money Laundering and Financing of Terrorism Policy

1 BACKGROUND AND OBJECTIVE

This policy applies to all employees at RiskPoint Group (the "Company") on a global basis. The objective of this policy is to state the requirements for business practices and personal conduct within the Company. All employees must be vigilant in order to protect the Company from participating in or being used for the purpose of money laundering and the financing of terrorism.

All employees are obliged to comply with applicate laws and regulations and this policy and all other relevant polices and guidelines in their daily work.

If applicable laws and regulation require higher standards than this policy, such standards must be followed.

2 WHAT IS MONEY LAUNDERING AND FINANCING OF TERRORISM?

Money laundering is a term used to describe the techniques, procedures or processes used to convert illegal funds obtained from criminal activities into other assets in such way as to conceal their true origin so that the profits appear to have originated from a legitimate source.

Transactions need not be cash transactions to constitute money laundering and money laundering can involve any movement of funds, cash and more. Fundamental stages of money laundering include the placement of criminal proceeds into the financial system, followed by the creation of layers of transactions designed to obscure the source.

Financing of terrorism utilizes many of the same processes in getting illicit funds in and out of legitimate financial systems. It is therefore closely connected to money laundering for regulatory purposes. It involves the provision, collection or receipt of funds with the intent or knowledge that the funds will be used to carry out an act of terrorism. It also includes collecting or receiving funds intending that they be used or knowing that they will be used for the benefit of a terrorist group.

While Anti-Money Laundering and Countering the Financing of Terrorism preventative measures often are dealt with together, it is important to note that a distinction exists in the nature of the two offences. For money laundering to occur, the funds must be the proceeds of criminal conduct. For terrorist financing to occur, the funds can be from a legitimate or illegitimate source.

3 COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM

Any employee who knowingly permits illegal conduct or turns a blind eye to suspicious activity indicating money laundering and the financing of terrorism will not only be subject to disciplinary actions by the Company, but may also subject themselves and the Company to criminal and civil penalties.

Money laundering issues are complex and should not be handled alone. If anyone becomes aware of any circumstances, which could suggest money laundering, or if anyone has any questions or concerns, they must promptly consult the Director of Finance & Operations.

Combatting any attempt to use the Company to launder money or financing terrorism rests on three pillars:

- Knowing Your Customer (KYC)
- Maintaining documentation
- Recognition and reporting of suspicious transactions

KYC is about getting to know who you do business with and is an integral part of all financial institutions' onboarding processes. Information such as legal name, legal structure, organisation ID, address and names of directors, as required by local law, must be obtained and saved as per local regulation. Steps should be taken to verify the customer's underlying beneficial owners, that is, those who ultimately own or control the customer. This is done through searches on publicly available records or as per local requirements.

Maintaining documentation helps determining if anything has changed at the customer year-over-year which could be a red flag. In addition, it also serves as evidence that the Company has complied with regulations. All documentation relating to the verification of the identity of the customer, as well as all records relating to each transaction, is retained for a period of seven years in readily retrievable form. Such records are maintained even after the customer relationship has been terminated.

Once a customer profile is set up in the internal system, it must be monitored for signs of money laundering and the financing of terrorism. Suspicions must be reported to the Director of Finance & Operations or through the Whistleblower reporting channel. Suspicious transactions include those inconsistent with a customer's known business or activities. Every occurrence must be filed in the **Financial Crime Log for Money Laundering cases.**

4 TIPPING OFF

In many jurisdictions it is an offence for a person to disclose information, likely to prejudice an investigation, where that information came to the person in the course of business in the regulated sector. If a customer has suspicious transactions, they may therefore not be notified of this.

5 ANTI-TAX EVASION

The Company conducts its business in accordance with all applicable financial crime and international economic, financial or trade sanctions laws and regulations. In addition RiskPoint Group has a zero tolerance approach to all forms of tax evasion under the laws of any country. Employees and Associates of RiskPoint Group must not undertake any transactions which they are aware will cause RiskPoint Group to commit tax evasion or facilitate tax evasion.

If any employee identify any such breaches in the course of our business or has concerns as to whether a transaction or arrangement could constitute tax evasion, they must promptly consult the Director of Finance & Operations. The Director of Finance & Operations will, as applicable, notify the relevant authorities and RiskPoint Group carriers.

6 SANCTIONS / PENALTIES

Failure to observe this Anti-Money laundering Policy is a cause for disciplinary action, including dismissal or summary dismissal, and may be reported to the relevant authorities.

7 COMMUNICATIONS AND TRAINING

All RiskPoint Group staff are obliged to complete Lloyds Coverholders - Financial crime prevention through E-Learning on Proceeds of Crime (including money laundering), Sanctions and Bribery. All employees are obligated to maintain their knowledge by completing the E-learning training every 2 years.

Version: 3
Dated: July 11th 2024