Hybrid XRMC DMCC Anti-Money Laundering (AML) Policy

UPDATED AS OF 4TH JANUARY 2023

1. Company Policy

It is the policy of the Company to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements under the Money Laundering Regulations in force in the UAE, including:

- **Federal Decree-Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations** (as amended by Federal Decree Law No. (26) of 2021
- **Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation** of Decree-Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations (as amended by Cabinet Resolution No. (24) of 2022).

In addition to all other relevant legislation in other legal jurisdictions where the Company operates or may operate in the future.

All directors, employees and consultants of the Company are under an obligation and duty to comply with the above. This policy & any related procedures aims to help partners and staff fulfil these responsibilities, by providing a clear framework, along with setting out the firm’s key principles and obligations.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Although cash is rarely deposited into securities accounts, the securities industry is unique in that it can be used to launder funds obtained elsewhere, and to generate illicit funds within the industry itself through fraudulent activities. Examples of types of fraudulent activities include insider trading, market manipulation, ponzi schemes, cybercrime and other investment-related fraudulent activity.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

Our AML policies, procedures and internal controls are designed to ensure compliance with all applicable regulations and rules and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

2. AML Compliance Person Designation and Duties

The firm has designated the Head of Legal as its Anti-Money Laundering Program Compliance Person (AML Compliance Person), with full responsibility for the Company's AML program. The head of legal has a working knowledge of the relevant legislation and its implementing regulations and is qualified by experience, knowledge and training.

The duties of the AML Compliance Person will include monitoring the firm's compliance with AML obligations, overseeing communication and training for employees. The AML Compliance Person will also ensure that the firm keeps and maintains all of the required AML records and will ensure that Suspicious Activity Reports (SARs) are filed with the Financial Crimes Enforcement Network (FinCEN) when appropriate. The AML Compliance Person is vested with full responsibility and authority to enforce the firm's AML program.

The firm will provide the local authorities with contact information for the AML Compliance, including: (1) name; (2) title; (3) mailing address; (4) email address; (5) telephone number; and (6) facsimile (if any). The firm will promptly notify the relevant authorities of any change in this information and will review, and if necessary update, this information within 10 business days after the end of each calendar year.

3. Giving AML Information to Law Enforcement Agencies and Other Financial Institutions

We will respond to any request by the authorities concerning any accounts and transactions by immediately searching our records to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity or organization named in the request. We understand that we have 14 days from the transmission date of the request to respond to a request.

Voluntary Information Sharing With Financial Institutions or Governmental Authorities

We will share information with financial institutions if requested by a relevant Government Authority or with the Authority directly regarding individuals, entities, organizations and countries for purposes of identifying and, where appropriate, reporting activities that we suspect may involve possible terrorist activity or money laundering.

We will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, for example, by segregating it from the firm's other books and records.

We also will employ procedures to ensure that any information received from another financial institution shall not be used for any purpose other than:

- identifying and, where appropriate, reporting on money laundering or terrorist activities;
- determining whether to establish or maintain an account, or to engage in a transaction; or
- assisting the financial institution in complying with performing such activities.

4. Our Commitment

We are aware of the risk of third parties exploiting us to engage in money laundering.

We do not assist, support, participate in or permit money laundering or terrorist financing.

We do not accept money or other assets if we know or suspect that they derive from any kind of criminal activity. We do not knowingly deal with criminals, suspected criminals or the proceeds of crime.

We do not facilitate the acquisition, ownership or control of criminal proceeds or other assets deriving from criminal activity nor do we assist others in concealing criminal proceeds or assets.

We do not tolerate tax evasion of any kind and we do not knowingly or willfully facilitate tax evasion. We implement procedures to prevent the facilitation of tax evasion by our people and others acting on our behalf.

To manage our money laundering risk exposure and ensure compliance, we implement a number of controls and processes. These include:

- conducting know your counterparty and due diligence procedures in order to determine the background and identity of our counterparties;
- implementing controls in respect of payments we make and receive using a risk-based approach to ensure that they are consistent with the requirements of this policy. For example, as a general rule, we make all payments under our contracts to, and receive payments from, our contractual counterparties to avoid the risk of facilitating money laundering or tax evasion;
- We require employees to be alert to any unusual or suspicious arrangements which could expose us to the risk of money laundering or the facilitation of tax evasion, and to report such arrangements to Compliance.

5. Whistle-blowing

The Company is responsible for ensuring that we meet our commitments. We expect our employees and contractors to speak openly and raise concerns about possible breaches of the Code of Conduct and this policy with their manager, supervisor or via other available reporting channels. Senior management is available to employees, contractors and external parties. Glencore takes concerns seriously and handles them promptly.

The Company has zero tolerance for retaliation against anyone who speaks openly about conduct they believe is unethical, illegal or not in line with our Code of Conduct and policies, even if the concern isn’t substantiated, as long as they have not knowingly made a false report.