Anti-Money Laundering and Anti-Terrorist Financing Policy

1. Purpose

The purpose of this policy is to implement an anti-money laundering and anti-terrorist financing program that is reasonably designed to prevent the Company from being used to launder money or finance terrorist or criminal activities. The Company is committed to:

- fostering a culture of conducting business with a high standard of integrity, honesty and ethics;
- complying with local, national and other applicable laws and regulations relating to anti-money laundering and anti-terrorist financing; and
- ensuring that the officers, employees, contractors, and agents ('**Personnel**') and businesses of the Company are well informed with respect to the Company's clients and counterparties and the nature of the transactions the Company engages in.

The above commitments are consistent with the Company's values of respect, integrity, teamwork, ownership and courage which guide the way we work, the way we treat each other and the standards we uphold to achieve the Company's purpose of creating value for our people, our communities and our shareholders by mining safely and responsibly.

In this policy, '**Company**' means Regis Resources Limited and its subsidiaries.

2. Scope

All Personnel of the Company are required to understand and comply with the terms of this policy. Employees are required to take practical steps to ensure contractors and agents of the Company are aware of this policy before entering into a contract with them.

Where local laws are more restrictive than this policy or other laws that might apply, Personnel must follow the more restrictive local law.

Questions regarding this policy should be directed to the Company's Company Secretary.

The remainder of this policy refers to the Company's anti-money laundering and anti-terrorist financing programs under the umbrella term '**AML Program**'.

3. AML Program

The Company's AML Program involves the development of internal policies, procedures and controls to prevent and detect money laundering.

The Company Secretary shall: (1) implement, administer and enforce this policy; (2) review and update this policy, as necessary, to comply with new laws or regulatory guidance; (3) evaluate the effectiveness of this policy; and (4) act as a liaison between Personnel and the Company regarding reporting suspicious activity and between the Company and law enforcement officials, government regulators, auditors and the media regarding this policy.

4. Understanding Money Laundering and Terrorist Financing

Money Laundering

Money laundering is generally defined as engaging in acts to conceal or disguise the true origin of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins. Money laundering typically occurs in three stages: (1) cash generated from illicit activity enters the financial system when converted into monetary instruments or deposited into accounts at financial institutions (the 'placement' stage); (2) the funds are transferred into other accounts or other financial institutions (the 'layering' stage); then (3) the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other legitimate or illegitimate activities (the 'integration' stage).

Terrorist Financing

Unlike money laundering, terrorist financing may not involve the proceeds of criminal conduct. Terrorist financing may come from legitimate sources such as charitable donations, foreign government sponsorship, business ownership and personal employment. Funding for terrorist attacks does not always require large sums of money, and the transactions associated with terrorist financing may not be complex. That said, terrorist financing can use the same methods as traditional money laundering.

Red Flags

The following is a non-exhaustive list of suspicious activities and transactions that could be evidence of illegal activity. and should be promptly reported to Company Secretary:

- A party insists on cash-only transactions;
- A party requests that funds be transferred to an unrelated third party in a transaction;
- A party is an agent or shell company and/or refuses to disclose the principal's or owner's identity;
- A transaction appears to have been structured to avoid government reporting requirements, including transmission of funds without normal identifying information or that attempt to hide or disguise the country of origin;
- Efforts by a party to cancel a transaction after being informed that verification and identifying information are required;
- Unusual concern or secrecy by a party with regard to identity, business or assets;
- A party lacks knowledge of its industry that it should obviously have to participate I that industry; and
- Refusal to make representations in connection with anti-money laundering and anti-terrorist financing. [***KWM note: we've amended this. There is some low level reluctance generally where parties are not familiar with the need for policies such as this***]

This list is indicative but is not exhaustive. Personnel should be vigilant as to other indicators that raise suspicion of illegal activity. When Personnel detect a red flag, they should notify the Chief

Compliance Officer. Under the direction of the Company Secretary, the Company will determine whether and how to further investigate the matter.

5. Checking Sanctions Lists and Know-Your-Client Procedures

Before entering into any material transaction or any transaction which is subject to a Red Flag, the Personnel involved must notify the Chief Compliance Officer and the Chief Compliance Officer will check to ensure that none of the parties involved in the transaction appear on any relevant sanctions lists, including but not limited to, the Specially Designated Nationals and Blocked Persons List ('**SDN List**') maintained and published by the Office of Foreign Assets Control ('**OFAC**'). To the extent necessary, the Chief Compliance Officer will seek advice from counsel for any clarity required in relation to the SDN List.

OFAC is an office of the U.S. Department of the Treasury that administers and enforces economic sanctions and embargoes based on US foreign policy and national security goals that target geographic regions and governments (e.g. Iran, North Korea, Cuba, Crimea), as well as individuals or entities that could be anywhere (e.g. terrorists, narcotics traffickers, proliferators of weapons of mass destruction). US persons are prohibited from dealing with SDNs where they are located, and all SDN assets must be blocked when they come into the possession or control of a US person or within US territory.

Although the purposes of such sanctions and embargoes extend beyond money laundering and counterterrorism, sanctions compliance is best performed in conjunction with anti-money laundering efforts. Because the SDN List and other sanctions lists are updated frequently, they must be consulted on a regular basis. Upon a member of Personnel determining or the Company otherwise becoming aware that a potential or existing client or counterparty is subject to US or other sanctions, or is engaging in transactions that are prohibited by US or other sanctions, the Company Secretary must immediately be notified.

In addition to sanctions checks, the Company requires that all clients and contract counterparties (including agents and contractors) shall be required to make certain representations relating to identity and compliance with applicable sanctions and anti-money laundering laws.

6. Breaches

Money laundering and terrorist financing are serious matters that represent a significant risk to the Company's operations and reputation.

Any breach of this policy by an employee will be investigated and may result in disciplinary action, including termination. For contractors and agents, a breach may result in action in accordance with the terms of the engagement or appointment, including termination of those services. The Company may report any breach of this policy to relevant authorities, including the police.

A breach of this policy may also expose both the individual who is in breach, as well as the Company, to criminal and civil liability under applicable anti-money laundering, anti-terrorist financing and sanctions laws which could result in significant penalties. Violations of such laws can also impact the Company's ability to continue doing business in a given country, region or market.

7. Reporting Suspicious Activity

The Company is committed to ensuring that money-laundering, terrorist financing and economic sanctions concerns can be raised without fear of reprisal or intimidation. Any employee who makes a bona fide disclosure under this policy and follows the reporting procedure in the Company's Whistleblower Policy will not be subject to any detrimental action by the Company as a result of making such a disclosure.

Any known or suspected breaches of this policy should be reported at the earliest opportunity to either the:

- Legal Counsel; or
- a Whistleblower Protection Officer.

8. Training

The Company will provide training to its Personnel about how to detect and report suspicious activity that could be linked to money laundering or terrorist financing. Company records related to the AML Program, including documentation of training, will be kept in accordance with the Company's recordkeeping policy.

Any Personnel who are uncertain as to any provisions of this policy or its application to a given circumstance should contact the Company Secretary.

9. Review

The Risk, Safety, Environment and Community Committee will monitor compliance with this policy and will undertake periodical review for the purpose of ensuring that it is operating effectively in light of the Company's then-current business activities and in accordance with any changes in applicable law. Any material amendments to the policy will be approved by the Board.