**GOMINING (BVI) LIMITED**

**AML/CFT COMPLIANCE Policy Version No. 1**

---

Gomining (BVI) Limited (the "**Company**") is committed to conducting its business with the highest ethical and legal standards. The Company has adopted this AML Compliance Policy (the **"Policy"**) to reduce the risk of money laundering and terrorist financing associated with its business and the sale of its products. The purpose of the Policy is to help detect and report suspicious activity including the predicate offenses to money laundering and terrorist financing.

---

## CHAPTER 1

## INTRODUCTION

### 1. PREAMBLE

1.1. Gomining (BVI) Limited (the "**Company**" or "**we**") is a professional mining company which has a fleet of devices conducting mining of BTC tokens (the **"Infrastructure"**), and as such the Company has created a digital platform and ecosystem (the "Platform") for the public to use the Company's Infrastructure and resources. Certain functionalities of the Platform can only be accessed through the Company native utility token "GMT".

1.2. The Clients include customers who access its services through the Platform. The Company's business is of a cross-border nature and accordingly, its Clients are based across the world.

1.3. The Company is incorporated under the laws of the British Virgin Islands.

### 2. THE BVI LEGAL FRAMEWORK

2.1. This section sets out some of the key provisions under BVI law relating to AML/CFT obligations but does purport to be exhaustive or up-to-date. It also does not reflect any rules and regulations that could apply to the Company outside of the British Virgin Islands. The Company undertakes to update the Policy to reflect any relevant changes to laws or regulations from time to time.

2.2. The legislation that applies to all persons in the BVI:

(a) In relation to money laundering is the Anti-Money Laundering Regulations (Revised 2020) ("**BVI AML Regulations**")[1];

(b) In relation to terrorism financing is the National AML/CFT Policy ("**BVI AML/CFT Policy**")[2].

2.3. The Company understands that the BVI AML REGULATIONS and the BVI AML/CFT POLICY impose substantive legal obligations that are not necessarily connected directly with CDD and apply to all businesses.

2.4. Each employee of the Company (the "Employee") should refer to the BVI AML/CFT POLICY to understand what constitutes a terrorist financing offence under the BVI AML/CFT POLICY, what the prohibitions are and what the duty to disclose entails in relation to terrorist financing. Unlike money laundering, the source of terrorist financing may be legitimate or illegitimate.

2.5. Employees must familiarize themselves with the BVI AML REGULATIONS and the BVI AML/CFT POLICY and comply with the same.

### 3. OTHER BEST PRACTICES FRAMEWORKS

3.1. Each Employee understands and acknowledges that there has been a lot of focus in recent times to the enhanced risk of transactions in cryptocurrency in recent years and accordingly, best practices and guidance in this space is evolving.

---

[1] https://www.bvifsc.vg/library/legislation/anti-money-laundering-regulations-revised-2020
[2] https://www.bvifsc.vg/fsc-amlcft-policies

3.2. In particular, a lot of attentions has been given by the Financial Action Task Force (FATF) which is the global money laundering and terrorist financing watchdog. The intergovernmental body sets international standards that aim to prevent these illegal activities and the harm they cause to society. As a policy-making body, the FATF works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas. The FATF has developed the FATF Recommendations, or FATF Standards, which ensure a coordinated global response to prevent organised crime, corruption and terrorism. They help authorities go after the money of criminals dealing in illegal drugs, human trafficking and other crimes. The FATF has noted that virtual currencies have emerged and attracted investment in payment infrastructure built on their software protocols. These payment mechanisms seek to provide a new method for transmitting value over the internet. At the same time, virtual currency payment products and services (VCPPS) present money laundering and terrorist financing (ML/TF) risks.

3.3. FATF made a preliminary assessment of these ML/TF risks in the June 2014 virtual currencies report (key definitions and Potential AML/CFT Risks). As part of a staged approach, the FATF has developed the "Guidance for a Risk-Based Approach to Virtual Currencies" (https://www.fatf-gafi.org/en/publications/Fatfgeneral/Guidance-rba-virtual-currencies.html) focusing on the points of intersection that provide gateways to the regulated financial system, in particular convertible virtual currency exchangers. FATF has stated that it will continue to monitor developments in VCPPS and emerging risks and mitigating factors to update this Guidance, to include, where appropriate, emerging best practices to address regulatory issues arising in respect of ML/TF risks associated with VCPPS.

3.4. This Guidance seeks to:

(a) Show how specific FATF Recommendations should apply to convertible virtual currency exchangers in the context of VCPPS, identify AML/CFT measures that could be required, and provide examples; and

(b) Identify obstacles to applying mitigating measures rooted in VCPPS's technology and/or business models and in legacy legal frameworks.

## 4. THE COMPANY'S OVERALL APPROACH

4.1. The Company's senior management has a zero-tolerance policy towards financial crime, money laundering and terrorist financing. The Company requires Employees to be vigilant for signs of financial crime and to immediately report any suspicious activities / incidents to the CO, who shall resolve and / or escalate such reports to the legal counsel of the company. The legal counsel shall, in turn, consult with the senior management team as appropriate.

4.2. The Company is committed to conducting its business in accordance with the highest ethical and professional standards in furtherance of the interests of its Clients and in a manner that is consistent with the spirit of all the laws, rules and regulations that generally apply to all businesses operating in the British Virgin Islands generally and to businesses dealing with cryptocurrency in particular, applicable laws in any other jurisdictions outside of the British Virgin Islands in which it conducts business and the evolving best practices standards in its industry from time to time while keeping in mind certain technological limitations that are unique to businesses that deal with cryptocurrency (the "**Standards**"). Except to the extent required by applicable law and regulation, the Company shall implement and adhere to the Policy and the Standards herein at its voluntary election in all respects. Given the Company

is incorporated in the British Virgin Islands, the Company pays particular attention to its obligations under the laws of the British Virgin Islands.

4.3. The Company shall implement the Policy and its policies herein utilizing a risk-based approach. As a best practice, the Company shall document instances in which it deviates from initial requirements of the Policy and utilizes a risk-based approach.

4.4. The Company may utilize the resources of third-party service providers ("**Service Providers**") in the implementation of the Policy.

4.5. The Company understands and acknowledges that while the Service Providers can assist with certain process aspects of administering the Policy, it remains responsible for complying with all relevant regulations under applicable law. Any references to the Company or its staff shall apply to the Service Providers of the Company or their respective staff to the extent elements of the Policy are performed by or outsourced to the Service Providers.

## 5. THE SCOPE OF THIS POLICY

5.1. The Company has adopted this Policy, which contains the policies and procedures to be adopted by the Company to help ensure compliance with the Standards. We expect the same from any Employees or independent contractors that we engage and from all officers and directors (collectively referred to as "**Officers**"). Accordingly, it is the responsibility of each of you to act at all times in a manner consistent with the Standards.

5.2. The interests of the Company and its Clients can be best served when all of the Employees are informed of the Standards and any legal requirements applicable to the business and understand the practices the Company has adopted to comply with those. Accordingly, this Policy is intended to achieve the following two objectives:

(a) To provide the Employees with an awareness of the applicable Standards and how they apply to the Company's activities; and

(b) To provide procedural means designed to ensure that the Company's operations meet the applicable Standards.

5.3. Employees shall be thoroughly familiar with all policies and procedures set forth in this Policy.

5.4. The Company has appointed the Compliance Officer (the "**CO**") of the Company. Any questions regarding compliance issues should be directed to the CO. The CO is responsible for assisting Employees and Clients in becoming familiar with the laws and regulations applicable to activities of the Company. The CO may hold compliance meetings and training sessions with all Employees to review any changes to the policies and procedures contained in the Policy.

## 6. EMPLOYEE ACKNOWLEDGEMENTS

6.1. When first employed by the Company, an Employee will be provided with a copy of this Policy. In addition, the CO may from time to time distribute to all Employees updated versions of the Policy. Employees are required to sign and return to the CO an acknowledgement form stating that they have received and comprehended the Policy and each subsequent material amendment, and that they have complied and will comply with all applicable policies and procedures contained in the Policy. The Compliance Acknowledgement Form is attached as Appendix 6 to this Policy.

6.2. Employees must complete the Compliance Acknowledgement Form and submit it to the CO:

(a) Within 14 (fourteen) days after first receiving this Policy, or as soon as reasonably possible thereafter; and

(b) Within 14 (fourteen) days upon receipt of an updated Policy, or as soon as reasonably possible thereafter.

6.3. The CO will maintain records of the Compliance Acknowledgement Forms.

## 7. CONSEQUENCE OF NON-COMPLIANCE

7.1. If an Employee fails to comply with the requirements of this Policy and all laws, rules, and regulations applicable to the Company's business, the Employee may be subject to disciplinary action by the Company, which may range from a letter of reprimand to termination of employment. Any non-compliance or violations of law also may result in severe civil and criminal penalties.

7.2. The Company also reserves the right to take disciplinary action against the Employee, including termination of employment, if the Employee engages in conduct deemed to be immoral, unethical, or illegal, regardless of whether such conduct constitutes a violation of the Policy or relates to the Company's business. The Company may take such action if, in our sole judgment, the Company believes that Employee’s conduct poses any reputational risk to the Company.

# CHAPTER 2

# AML / CFT / SANCTIONS POLICY

## 8. GENERAL DESCRIPTION OF MONEY LAUNDERING

8.1. Criminal proceeds are where criminals generate profit by illicit acts such as illegal arms sales, smuggling, activities of organised crime, including for example, drug trafficking and prostitution rings, embezzlement, insider trading, bribery and computer fraud schemes.

8.2. The Company understands money laundering is the act of engaging in specific financial transactions with the intention of concealing the identity, source and / or destination of the criminal proceeds. Money launderers act to alter the identity of the source of criminal proceeds to create the appearance that it originates from a legitimate source. The most common way in which this is achieved is by giving these proceeds to an intermediary who is already legitimately taking in large amounts of cash. Being completely fungible, cash is easily the preferred medium of exchange in the criminal world.

8.3. There are three stages in the process of money laundering, namely:

(a) Placement or moving the cash proceeds from direct association with the illegal activities;

(b) Layering or disguising the trail to prevent detection. This pertains to the separation of criminal proceeds from their sources by creating complex layers of financial transactions designed to disguise the financial sources where the proceeds came from, subvert the audit trail and provide anonymity (because capital markets are no

longer predominantly cash based, it is more likely to be used in the layering stage of money laundering); and

(c) Integration or making the money available to the criminal, once again, with its occupation and geographic origins hidden from view. This creates the impression of apparent legitimacy of criminally derived wealth. In the event where the layering process is successful, integration schemes effectively return the laundered proceeds back into the financial system as if the proceeds were from legitimate business actions.

## 9. GENERAL DESCRIPTION OF TERRORISM FINANCING

9.1. The Company understands that terrorist financing refers to the carrying out of transactions involving funds or property that are owned or controlled by terrorists or terrorist organisations or transactions that are linked to or likely to be used in terrorist activities. Terrorists or terrorist organisations require financial support in order to achieve their aims. There is often a need for them to obscure or disguise links between them and their funding sources. Therefore, the terrorist groups must find ways to launder funds regardless of whether the funds are from an illicit or legitimate source in order to be able to use them without attracting the attention of law enforcement agencies.

## 10. GENERAL DESCRIPTION OF ECONOMIC SANCTIONS

The Company fully adheres to and complies with the sanctions which are imposed or may be imposed by the BVI Government or by the Financial Services Commission (**"FSC"**), as the case may be. The list of the sanctions which are in place as of the date hereof is available at

https://www.bvifsc.vg/sanctions-regime

10.1. In addition to the UK sanctions, depending upon the particular facts and circumstances, U.S. primary sanctions may apply to certain Company activities and U.S. secondary sanctions must be considered with respect to all Company activities, even those not otherwise subject to U.S. jurisdiction. As such, in addition to the obligations imposed on the Company by virtue of it being a BVI company, we have elected to adopt measures to comply with sanctions promulgated by the United States, which are discussed in further detail below.

10.2. U.S. sanctions generally apply to U.S. persons, defined to include both individuals and entities, wherever located. They also apply to conduct occurring within the United States by non-U.S. persons, including in situations in which a non-U.S. actor causes another person to violate U.S. sanctions.

10.3. As part of its duty to implement and enforce U.S. sanctions programs, the Office of Foreign Assets Control ("OFAC") maintains lists of individuals and entities with whom U.S. persons, and persons acting within the United States, may not do any business, or may not do certain business, absent specific authorization from OFAC. Dealing with such persons may also be sanctionable for non-U.S. persons in a variety of circumstances even when acting entirely outside of the United States.

10.4. Although each of the more than 20 sanctions programs administered by OFAC is unique, they all generally involve cutting off access to the U.S. marketplace by prohibiting transactions in certain property (or interests in property) within the U.S. or involving U.S. persons, and/or requiring U.S. persons to block (i.e., freeze) the property of those listed on OFAC's list of Specially Designated Nationals and Blocked Persons (the ''SDN List''). Though not specifically listed in the OFAC SDN List, designations extend to entities that are 50% or more

owned, directly or indirectly, by persons on the SDN List (whether alone or in conjunction with other listed persons). As noted above, it may also be sanctionable for non-U.S. persons to deal with SDNs even if such dealings are entirely outside the United States.

10.5. In accordance with this Policy, the Company and all Employees are prohibited from engaging in any business or transaction with any individual or entity on the OFAC SDN List, and any entity 50% or more owned by an individual or entity on the SDN List.

10.6. In addition to the SDN List, the U.S. government maintains a variety of other sanctions and restrictive trade lists such as the Sectoral Sanctions Identifications List and the Entity List, among others. It is Company policy not to deal with persons contained on such lists absent guidance from U.S. counsel that the contemplated activities are not prohibited or otherwise sanctionable for the Company and other associated persons.

10.7. In addition to the targeted sanctions discussed above, the U.S. maintains comprehensive embargoes against a number of jurisdictions, currently, Iran, Cuba, North Korea, Syria, Myanmar, the Crimea region of Ukraine, and the so-called Donetsk People's Republic (DNR) and Luhansk People's Republic (LNR) regions of Ukraine. Dealings with such jurisdictions are generally prohibited for U.S persons or persons acting within the United States and non-U.S. persons may be subject to secondary sanctions for certain dealings involving those jurisdictions. It is against Company policy to conduct any business with jurisdictions subject to comprehensive embargoes, including with the government of such jurisdictions and with persons or entities located in such jurisdictions, incorporated in such jurisdictions, or owned by individuals in such jurisdictions.

10.8. OFAC has also imposed sector-based sanctions, including secondary sanctions, against certain countries, including Russia and Venezuela. The Company must carefully review any dealings with such countries to ensure they are not prohibited or otherwise sanctionable under U.S. law. The Compliance Officer shall be responsible for making any such decisions.

10.9. Should the Company be in the possession of property or interest in property of an SDN or another person considered blocked under the sanctions laws of the U.S., the Company shall freeze the property of such person and document such freezing. For digital assets, the Company shall place the digital assets in a segregated cold storage wallet, separate from the assets of the Company and any other Company customers.

10.10. The private key associated with that wallet shall be held in a secure location as determined by the Compliance Officer. The digital assets shall remain in that wallet until such time as the person is no longer included on the applicable sanctions list. Because the Company is not a U.S. person or person subject to U.S. jurisdiction for purposes of OFAC's reporting requirements, it is not required to file blocked property or rejected transaction reports with OFAC. However, the Compliance Officer in conjunction with company counsel may decide that a report to OFAC or another governmental agency is warranted or required based on the particular facts and circumstances.

## 11. AML / CFT / SANCTIONS RISKS IN RELATION TO CRYPTOCURRENCIES

11.1. The legitimate use of cryptocurrencies offers many benefits such as increased payment efficiency and lower transaction costs. However, the Financial Action Task Force ("**FATF**") has highlighted that the characteristics of cryptocurrencies, coupled with their global reach, present the following AML / CFT risks:

(a) The anonymity provided by the trade in cryptocurrencies on the Internet;

(b) The limited identification and verification of participants;

(c) The lack of clarity regarding the responsibility for AML / CFT compliance, supervision and enforcement of these transactions that are segmented across several countries; and

(d) The lack of a central oversight body.

## 12. PRIMARY AML / CFT / SANCTIONS RESPONSIBILITIES

12.1. The Company adopts the following two primary responsibilities in relation to AML / CFT / Sanctions matters:

(a) Conducting its business in conformity with high ethical standards and guarding against undertaking any transaction that is or may be connected with or may facilitate money laundering, terrorist financing, or economic sanctions violations, including the monitoring of possible suspicious transactions; and

(b) Whenever and to the fullest extent possible, assist and cooperate with the relevant law enforcement authorities in the British Virgin Islands and elsewhere (where applicable) in preventing money laundering, terrorist financing, and economic sanctions violations, as well as monitoring and reporting any suspicious Clients or activities.

12.2. To mitigate the money laundering, terrorism financing, and economic sanctions risks identified herein, the Company shall:

(a) Develop and implement policies, procedures and controls, which are approved by the senior management, for the Company to effectively manage and mitigate the risks that have been identified by the Company or notified to it by any relevant regulatory authorities;

(b) Monitor the implementation of those policies, procedures and controls and enhance them if necessary;

(c) Perform enhanced measures where higher risks are identified, to effectively manage and mitigate those higher risks; and

(d) Ensure that the performance of measures or enhanced measures to effectively manage and mitigate the identified risks address the risk assessment and guidance issued by the relevant authorities from time to time.

# CHAPTER 3

# CLIENT ONBOARDING

## 13. THE COMPANY'S APPROACH TO ONBOARDING

13.1. The Company is responsible for the verification of the identity of its Clients. For its internal purposes, the Company has defined a "**Client"** to be a person (whether a natural person, legal person or legal entity) with whom the Company:

(a) Establishes or intends to establish business relations with;

(b) Who undertakes or intends to undertake any service from the Company; or

(c) Undertakes or intends to undertake any transaction, on the Company's digital platform (the "**Platform Customer**").

13.2. The Company must also take reasonable measures to verify the identities of the beneficial owners of its Clients, including the underlying investors and / or controllers of the Company, or if the Client is a fund, the party who act as fund manager.

13.3. For the purposes of a Platform Customer, "beneficial owner" means the natural person who ultimately owns or controls the customer or the natural person on whose behalf a transaction is conducted or business relations are established, and includes any person who exercises ultimate effective control over a legal person or legal arrangement.

13.4. The Company has reviewed and will periodically re-assess the arrangements that underlying investors have in place in relation to the prevention of money laundering. The oversight of this process is led by the CO.

## 14. CONDUCTING CLIENT DUE DILIGENCE ("CDD")

14.1. CDD shall be conducted on each prospective Client before entering into business relations with such prospective Client.

14.2. The Company takes the following measures to conduct CDD:

(a) Gathering CDD data from prospective Clients including such additional information deemed appropriate after the Company has reviewed the preliminary data received;

(b) Reviewing the CDD data collected;

(c) Conducting the simplified CDD as per Paragraph 16;

(d) If required, conducting enhanced CDD as per Paragraph 17 below;

(e) Based on the foregoing, approving or rejecting the prospective Client's application to be onboarded as a Client, as well as documenting such approval or rejection and the basis for such decision.

14.3. Where irregular data, information or any anomalies arise in the course of the CDD, the Company shall not share any such anomalies of the CDD with Clients (other than a statement notifying the prospective Client that he / she has not satisfied the Company's onboarding requirements.

14.4. In the event business relations are established prior to completion of the Company's CDD procedures, the reasons and process for managing money laundering and terrorist financing risks shall be documented and approved by the CO.

14.5. At this time, the transactions with Platform Customers are considered most high-risk for the Company relative to its other business activities and therefore this section of Policy focusses on AML/CFT procedures followed for Platform Customers.

## 15. BASIC CLIENT INFORMATION REQUIRED

15.1. In all cases, the Company will obtain the following information from prospective Clients who are Platform Customers (the "**Basic Information**"):

(a) Identity verification in the form of a photo of the client (which would be in the form of a "selfie" in an approved format);

(b) The Client's name;

(c) Date and place of birth (if Client is a natural person), or date and place of incorporation or registration (if Client is a legal entity);

(d) Primary citizenship;

(e) Gender (if Client is a natural person);

(f) Email address;

(g) Residential address;

(h) Proof of a current residential address or proof of a current registered entity address (such as a bank statement, electricity or water bill issued within the last three months); and

(i) If the Client is a natural person, proof of identification with a photograph in the form of a passport (which shall include a unique identification number, such as a passport number) or, if permitted, another document such as an identity card or a birth certificate number. If the Client is a legal entity, proof of registration or incorporation (such as a certificate of incorporation or registration, which shall include a unique entity number).

## 16. RISK-SCORING APPROACH

16.1. For Platform Clients who are subject to CDD procedures as above, the Company will conduct identity verification and KYC checks. The Company conducts identity verification and KYC checks through the process set out in the process flow attached hereto as Appendix 7 hereto and under which:

(a) The Company seeks the assistance of Service Providers for the identity verification and other KYC checks through an API linking to the Company's platform; and

(b) The CO thereafter manually approves or declines each transaction or asks for more information from the Client.

16.2. In general, CDD comprises the following activities:

(a) Identifying the prospective Client by obtaining certain information; and

(b) Verifying the identification information obtained.

16.3. The Company applies a risk-assessment process to assess the risk profile of a prospective Client for the purposes of determining the level of CDD. Appendix 1 hereto sets out certain resources that the Company will use to determine country specific risks and Appendix 2 sets out the Company's current determination of "**Current High-Risk and Prohibited Countries**" (which is updated from time to time) based on specific inherent risks and prohibitions that

may change over time. Each country listed in Appendix 2 is a "**High-Risk or Prohibited Country**" and the Company shall decline to conducted business with any Clients located in such jurisdictions, including entities incorporated in, operating from, or beneficially owned by persons located in such countries. The Company has also noted that the following countries are generally perceived to have a relatively higher AML/CFT risks: Afghanistan, Haiti, Myanmar, Laos, Mozambique, Sierra Leone, Senegal, Kenya, Yemen and may be more likely to subject to Clients from those countries to enhanced CDD.

16.4. Given that the Company's business has a nexus to cryptocurrencies, as part of the CDD process, it may also conduct certain checks on the address used by a Platform Client for receiving or transmitting funds. For this purpose of conducting checks on the address, it may request a Service Provider for assistance from time to time.

16.5. The Company will also base its risk assessment on such local or international resources that become available from time to time. One such resource is the Virtual Assets Red Flag Indicators of Money Laundering published by the FATF in September 2020 (https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html) which highlighted the following risks in particular:

(a) Technological features that increase anonymity - such as the use of peer-to-peer exchanges websites, mixing or tumbling services or anonymity-enhanced cryptocurrencies;

(b) Geographical risks - criminals can exploit countries with weak, or absent, national measures for virtual assets;

(c) Transaction patterns - that are irregular, unusual or uncommon which can suggest criminal activity;

(d) Transaction size – if the amount and frequency has no logical business explanation;

(e) Sender or recipient profiles - unusual behavior can suggest criminal activity; and

(f) Source of funds or wealth - which can relate to criminal activity.

## 17. ENHANCED CDD

17.1. Enhanced CDD may be required for a Client if:

(a) The Client or any natural person appointed to act on behalf of the Client, any connected party to the Client or any beneficial owner of the Client is a PEP (as described in greater detail in Appendix 4), or a family or close associate of a PEP; or

(b) Were any other red flags or potential red flags arise during the onboarding process.

17.2. An Employee must undertake the following additional steps as part of enhanced CDD:

(a) Obtaining approval from the Company's senior management (CO) to establish or continue business relations with the prospective Client;

(b) Establishing the source of wealth and source of funds of the Client and any beneficial owner of the prospective Client; and

(c) Conducting, during the course of business relations with the Client, enhanced monitoring of business relations with the Client. In particular, the Employee handling the Client's matters shall increase the degree and nature of monitoring, in order to determine whether the transactions and / or activities appear unusual or suspicious.

17.3. In cases which require enhanced CDD, the Company will require the prospective Client to provide either original or certified copies of the items Paragraph 15.1 (h) and (i). Certified documents must be certified by a qualified third party such as a notary public. The certifier must sign and date the copy document (printing his / her name clearly in capitals underneath) and clearly indicate his / her position or capacity on it and provide his / her contact details. The certifier must also state that it is a true copy of the original document. The completion of this exercise will be documented by the CO.

17.4. In the event the enhanced CDD is successfully completed and the review by the Service Provider (if any) does not yield any anomalies and the CO is satisfied that there is no AML/CFT/sanctions risk in relation to the Client, the Company may establish business relations with the prospective Client.

17.5. In the event the review by the Service Provider yields any anomalies, the application of the prospective Client to establish business relations with the Company will be provisionally declined (subject to a further review by CO, which may include further procedures being undertaken).

## 18. PROHIBITED JURISDICTIONS

18.1. The Company has determined that it will not engage in any business relationships with Clients located in certain jurisdictions where such conduct may expose the Company to legal risk or is otherwise considered high risk. These jurisdictions are enumerated in the list of High Risk and Prohibited Countries in Appendix 2. This restriction applies to individuals as well as entities that are organized in, operating from, or have beneficial owners located in such jurisdictions. In order to ensure the Company does not engage in business relationships with such persons it has taken a number of steps:

(a) The Company has implemented a Platform Customer onboarding process, which includes a robust KYC process, including collection of a governmental ID and proof of address;

(b) The Company has implemented IP geoblocking such that persons located in prohibited jurisdictions are unable to access the Platform or see the website;

(c) The Company uses blockchain analytics through a Service Provider that look for wallets known to be associated with prohibited jurisdictions;

(d) The Company makes clear on its website, including in its terms of service, that it does not service persons located in a prohibited jurisdiction.

## 19. SCREENING CHECKS BY SERVICE PROVIDERS

19.1. As part of the basic CDD checks, the Service Provider will, upon receiving the Basic Information, screen each prospective Client against its databases for the compliance matters referred to therein.

19.2. In the event of a screening hit, the Company will exercise its discretion and judgement to determine whether the prospective Client should continue to be treated as a high-risk Client, having regard to the risks and circumstances of each case. The Company may decide to conduct enhanced CDD in accordance with Paragraph 17 on the prospective Client, conduct additional procedures or escalate the case to the CO for a decision as to whether the Company will onboard the prospective Client.

19.3. The rationale for approving a prospective Client with the presence of such a screening hit shall be documented pursuant to Paragraph 14.2 (e) above.

19.4. In addition to the prospective Client's high-risk status, factors such as the age and nature of a screening hit may be considered to present a greater or lesser risk of money laundering and terrorist financing. Attention will be paid to membership applications and transactions with Clients from or residing in countries that have inadequate AML / CFT measures.

19.5. The Company will liaise with the Service Provider to ensure that the additional checks are adequate, and upon request, the Service Provider will provide the Company with the list of databases that the Service Provider uses for screening.

19.6. While the Company remains responsible for conducting these checks, it uses the help of Service Providers from time to time to conduct the checks as detailed in Paragraph 4.4(b) above.

## 20. MONITORING AND SUSPICIOUS TRANSACTION REPORTING

23.1. The Company will monitor, on an ongoing basis, its account relationships with its Clients. The Company will observe the conduct of the Clients' account and scrutinise transactions undertaken throughout the duration of the business relations to ensure that the transactions are consistent with the Company's knowledge of the Client, the risk profile and, where appropriate, the source of the Clients' funds.

23.2. Employees should pay special attention to all complex, unusually large or unusual patterns of transactions undertaken throughout the course of the business relations, particularly any transactions that have no apparent or visible economic or lawful purpose.

23.3. Therefore, if an Employee has observed that a particular Client has been deemed to be of "High Risk" under the criteria set out in the Risk Detection Scenarios Table set out in Appendix 3, then the Employee must report to the CO.

## 21. SUSPICIOUS TRANSACTION REPORTING

24.1. If you are suspicious about a Client, you should as a first step request more information from the Client. You must decide if the explanation received is reasonable and legitimate and if not, you should report the transaction to the CO, who shall also be the Company's designated officer in charge of AML / CFT matters who shall be the CO for the time being. In the future, the Company may appoint a dedicated officer as the "**AML / CFT Officer**" who shall act in place of the CO in relation to the specific responsibilities identified herein. A template of the report which you may submit to the CO is attached hereto as Appendix 5.

24.2. The following are some relevant factors (though not exhaustive) that an Employee should be mindful of when seeking to identify a suspicious transaction or activity:

(a) Is the Client known personally;

(b) What is the Client's economic / financial status, employment history, behavior and general background;

(c) Does the transaction or activity make sense for that particular Client;

(d) Are the transactions in keeping with the normal practice in the market to which it relates, with reference to the market, size and frequency;

(e) Is the transaction to be settled in the normal manner;

(f) Is the role of any agent involved in the arrangement unusual;

(g) Are the reasons for the transaction or activity transparent and understandable, or is there a cheaper, easier or more convenient method available, which the Client appears to be avoiding;

(h) Are the Client's instructions structured in such a way that the economic or lawful purpose of the instruction is not apparent or is absent entirely;

(i) When asked to explain the circumstances or the transaction, is the Client evasive or gives explanations which do not stand up to reasonable scrutiny?

## 22. TIPPING-OFF

22.1. It is critical that the Employees do not:

(a) Express their suspicion within earshot of others;

(b) Discuss the matter with any of their colleagues, including their manager, either before or after notification; and

(c) Discuss the matter with the Client or any of his / her affiliates or professional advisers.

Any of the above could cause an Employee to commit the offence of "tipping off" which may result in a criminal conviction.

## 23. REFRESHER CDD

23.1. It is a basic requirement that CDD information be kept up to date. If a Client wishes to update its CDD information or the Company becomes aware that the CDD information is out-of-date, the CO will initiate the risk assessment procedure in Paragraph 16 prior to any new transaction or activity with such Client. It is noted that the Service Providers of the Company will update the KYC checks conducted on the Platform Clients at certain periodic intervals and the results of these checks shall be escalated to the CO for further action if required.

23.2. In addition, the Company will require the Clients to undergo mandatory refresher CDD on a periodic basis. At a minimum:

(a) Clients who were approved on the basis of simplified CDD in Paragraph 16 above will undergo a refresher CDD every three years;

(b) Clients who were approved on the basis of enhanced CDD in Paragraph 17 above will undergo a refresher CDD every year.

## 24. TRAINING

24.1. The CO will ensure that appropriate levels of training are provided to all Employees. The CO will decide on the training to be provided for the Employees on an annual basis, including the subject matter, delivery method and timing. A record of the training completed by each Employee shall be kept by the CO. An annual review of the Company's operations will be undertaken by the CO to see if certain Employees require specialized additional training.

24.2. All Employees of the Company must attend training in relation to AML / CFT at least once every two years.

24.3. The CO shall monitor the effectiveness of the training provided to the Employees. This may be achieved by:

(a) Testing the Employees' understanding of the Company's policies and procedures to combat money laundering and terrorism financing, their obligations under relevant laws and regulations, and their ability to recognise suspicious transactions;

(b) Monitoring the Employees' compliance with the Company's AML / CFT policies, procedures and controls as well as the quality and quantity of internal reports so that further training needs may be identified, and appropriate action taken; and

(c) Monitoring attendance and following up with the Employees who miss such training without reasonable cause.

24.4. The CO shall conduct periodic training for the Employees regarding the reporting structure and process in the event of receiving an inquiry from a regulatory authority (as described in Paragraph 27 below) to ensure accurate and timely provision of information to the competent authority or authorized officer.

24.5. In addition to the above, Employees who are acting in the capacity of a Company representative shall undertake continuous education to keep abreast of developments (in particular, regulatory developments) and enhance their professionalism in the industry.

24.6. The senior management shall ensure that:

(a) Employee training needs are assessed at the outset and at regular intervals (or when their roles change);

(b) Training and support are provided to ensure satisfaction of any prevailing or applicable industry regulation;

(c) Regular reviews of the training are conducted;

(d) Technical knowledge, skills, expertise and changes in market requirements and regulations are taken into account; and

(e) Adequate records are maintained at all times for at least five years after the Employee ceases to carry on the relevant activity for the Company.

## 25. RECORD KEEPING

25.1. The CO must:

(a) Ensure that documents are kept such that any individual transaction can be reconstructed (including the amount and type of currency involved) so as to provide, if necessary, evidence for prosecution of criminal activity;

(b) Comply with the record retention periods:

i. For CDD information relating to the business relations, the account files and business correspondence, a period of at least five years following the termination of such business relations or completion of such transactions;

ii. For data, documents and information relating to a transaction, a period of at least five years following the completion of the transaction;

(c) Retain data, documents and information as originals or copies, in paper or electronic form or on microfilm, provided that they are generally admissible as evidence in a court of law;

(d) Retain records of Clients or transactions for a Client pertaining to a matter which is under investigation or which has been the subject of an STR, or order from any competent regulatory authority; and

(e) Keep records of all transactions referred to the competent regulatory authority, together with all internal findings and any related analysis done.

25.2. CDD records shall be maintained for a minimum of seven years after the later of:

(a) A Client's onboarding; or

(b) A rejection of a prospective Client's application to establish business relations with the Company or the termination of such relations.

25.3. The Company shall comply with applicable law regarding the storage and safekeeping of CDD records.

25.4. If the KYC records of the Company are kept by the Service Providers, the CO shall ensure that it has access to such records as and when required.

## 26. ONGOING REVIEW AND ANNUAL REVIEW

26.1. The CO shall review this Policy on a need basis but at least one time per year in order to:

(a) Incorporate any changes to legislation which may affect how the Company operates;

(b) Consider benchmarks and best practice reviews; and

(c) Reflect the outcome of the annual risk assessment.

26.2. The Company will also consider ongoing developments in AML / CFT on a regular basis and review this Policy and the policies and procedures herein in light of such developments to determine if amendments are required to the Policy. The Company has also noted that there are new and emerging risks for cryptocurrency from time to time. As an example, the US Department of the Treasury's Office of Foreign Assets Control ("OFAC") has recently issued

an updated advisory to highlight the sanctions associated with ransomware payments in connection with malicious attacks on digital platforms.

## 27. RESPONDING TO INQUIRIES FROM REGULATORY AUTHORITIES

27.1. The Company operates in a number of jurisdictions which regard cryptocurrency transactions as high-risk. There may be inquiries from a variety of governmental and regulatory agencies.

27.2. If you are contacted by a government official or other industry regulator or exchange, whether by telephone, letter or office visit, you may not, under any circumstances, engage in discussions with the contacting party, or take any other action in response to such contact, other than:

(a) Advising the contacting party that all Employees are under instructions to refer all such inquiries to the CO; and

(b) Promptly notifying and forwarding any documentation received to the CO unless you are prohibited by law from doing so.

27.3. Employees should not contact government officials or regulators directly unless authorised to do so by the CO. These obligations shall exist throughout your employment with the Company and at all times following your leaving the Company's employment.

27.4. The provisions in this Paragraph 27 do not apply to lawful communications, other than on behalf of the Company, with any governmental or regulatory body or official regarding a possible violation of any fair employment practices law. You have the right to contact any such agencies or persons for such purposes.

27.5. All documentation and correspondence with government officials or regulators will be kept by the CO, on behalf of the Company. Employees must not destroy any documentation evidencing dealings with or reporting to government officials or regulators unless approved by the CO. Such records are confidential and should not be disclosed or made accessible or available to third parties whether in or outside the Company.

## 28. REPORTING OF NON-COMPLIANT ACTIVITIES AND WHISTLE-BLOWING

28.1. Employees must report to the CO of any known or suspected violations of the Policy and the policies and procedures herein, or other activities of any Employee that could be construed as a violation of the Standards or any law, rule or regulation applicable to the Company's business.

28.2. It is important to note that in many jurisdictions, an Employee's obligations to report suspicious activity are not tied to knowledge of an actual act or a confirmation by the Employee that the activity is in fact a violation of the Standards or illegal. Rather, such obligations are tied to "reasonable suspicions" that such an activity is occurring. If you are unsure whether a violation has occurred, you should discuss the matter with the CO.

28.3. Failure to report a violation to the CO could result in disciplinary action against any non-reporting Employee, which may include termination of employment. The Company has a non-retaliation policy that applies to Employees who report such matters in good faith.

## Appendix 1

## COUNTRY RISK CLASSIFICATION - ADDITIONAL RESOURCES

The Company will consider the following lists:

- FATF's website link of jurisdictions under increased monitoring: https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-october-2022.html
- BASEL AML Index: https://www.baselgovernance.org/basel-aml-index
- Corruption Perception Index by Transparency International: https://www.transparency.org/en/cpi#

Lists relevant to terrorist financing include:

- The List established and maintained by the Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning ISIL (Da'esh) Al-Qaida and associated individuals groups undertakings and entities: https://www.un.org/securitycouncil/sanctions/1267;
- The List established and maintained by the Committee established pursuant to resolution 1988 (2011) with respect to individuals, entities, groups, or undertakings https://undocs.org/S/RES/1988(2011)

For risk countries in the context of tax crimes, the Company also refers to:

- Global Forum on Transparency and Exchange of Information for Tax Purposes: https://www.oecd.org/tax/transparency/
- Financial Secrecy Index by Tax Justice Network: https://www.taxjustice.net/

## Appendix 2

## CURRENT HIGH-RISK AND PROHIBITED COUNTRY LIST

The Company has concluded that having clients in the following countries would be either prohibited under applicable law or otherwise high risk to the Company. Therefore, the Company will not establish business relationships with any clients located in such countries, including entities organized, operating from, or beneficially owned by persons located in such countries. Those countries include:

- Cuba
- North Korea
- Iran
- Syria
- The Crimea Region of Ukraine
- The so-called Donetsk People's Republic (DNR) and Luhansk People's Republic (LNR) regions of Ukraine
- The People's Republic of China
- Singapore
- Myanmar

## Appendix 3

## RISK DETECTION SCENARIOS TABLE

### Incoming Payments

| Type | Scenario Name | Scenario Description |
|---|---|---|
| Incoming Transaction | Transaction Risk - Predicate Offences | Transaction associated with certain predicate offences. |
| Incoming Transaction | High Geographic Risk | Transaction activity from high-risk geographic location without an apparent business reason. |
| Incoming Transaction | Incoming Transaction Amount Above Threshold | Incoming transaction amount above preset threshold (USD 10K) |
| Incoming Transaction | Aggregated Incoming Transaction Amount Above Threshold (14 days) | Incoming transaction amount over a preset period above pre-set threshold (USD 50K) |
| Incoming Transaction | Aggregated Incoming Transaction Amount Above Threshold (30 days) | Incoming transaction amount over a pre-set period above pre-set threshold (USD100K) |

### Outgoing Payments

| Type | Scenario Name | Scenario Description |
|---|---|---|
| Outgoing Transaction | Address Risk - Predicate Offences | Receiving address associated with certain predicate offences. |
| Outgoing Transaction | High Geographic Risk | Receiving address has transaction activity from high-risk geographic location without an apparent business reason. |
| Outgoing Transaction | Outgoing Transaction Amount Above Threshold | Outgoing transaction amount above preset threshold (USD 10K) |
| Outgoing Transaction | Aggregated Outgoing Transaction Amount Above Threshold (14 days) | Outgoing transaction amount over a preset period above pre-set threshold (USD 50K) |

## Appendix 4

## DEFINITION OF POLITICALLY EXPOSED PERSON ("PEP")

### 1. RISKS

PEPs present increased money laundering, corruption and reputational risk to financial institutions due to their position or influence. The primary risk associated with business relationships with PEPs is that they may use accounts that they control to conceal funds or assets that have been misappropriated as result of abuse of official position or resulting from corruption.

### 2. DEFINITION

2.1. A PEP is a natural person who are or have been entrusted with prominent public functions and the immediate family members, or individuals known to be close associates, of such persons.

2.2. The following is a non-exhaustive list of functions that would classify an individual as a PEP:

(a) Heads of state, heads of government, President, Prime ministers;

(b) Ministers on a national level and deputy or assistant minister;

(c) Governors of states or provinces;

(d) Members of national parliaments;

(e) Members of the governing bodies of political parties;

(f) Executive members of the administrative, management or supervisory bodies of state-owned companies and enterprises;

(g) High-ranking transaction participant of the military;

(h) High-ranking officials in the national administration;

(i) Officer or judge of supreme courts, of constitutional courts or of other high-level judicial bodies;

(j) Member of statutory boards of central banks;

(k) High-level diplomats;

(l) High-level representatives of religious organisations (if their functions are linked to political responsibilities);

(m) Persons who are or have been entrusted with prominent function in international sport associations;

(n) Persons who are or have been entrusted with a prominent function by Inter-governmental organisation (e.g., Secretary General of the United Nations).

**Appendix 5**

**FORM OF SUSPICIOUS TRANSACTION REPORT**

Attention: Compliance Officer, GOMINING (BVI) LIMITED.

| Part 1: Information on Employee Filing Report | |
|---|---|
| Name of employee filing | |
| Designation of employee filing report | |
| Email of employee filing report | |
| Contact no. of employee filing report | |
| **Part 2: Relationship Between the Company and Client Subject to This Report** | |
| Name of Client subject to this report | |
| Date of establishment of relations | |
| **Part 3: Suspicious Transaction(s)** | |
| Total amount involved in the suspicious transactions (USD) | ☐ No amount involved<br>☐ 0 to < 20,000<br>☐ 20,000 to < 100,000<br>☐ 100,000 to < 500,000<br>☐ 500,000 to < 1,000,000<br>☐ 1,000,000 to < 10,000,000<br>☐ 10,000,000 to < 30,000,000<br>☐ 30,000,000 to < 50,000,000<br>☐ 50,000,000 or more<br>☐ Unknown |

| | |
|---|---|
| Possible type of crime | ☐ Terrorism and threats to security<br>☐ Tax crimes and smuggling<br>☐ Fraud / cheating<br>☐ Money laundering<br>☐ Organised crime and racketeering<br>☐ Securities-related offences<br>☐ Environmental crime<br>☐ Robbery, theft and other serious violent crimes |

| | |
|---|---|
| | ☐ Trafficking of humans, smuggling of migrants, sexual exploitation, including exploitation of children<br>☐ Counterfeiting and piracy of products<br>☐ Bribery / corruption-related<br>☐ Drug-related offences<br>☐ Unknown |
| Reason for suspicions | |
| Signature of employee filing report | |
| Date of submission of report | |
| Part 4: Follow-Up by Compliance Officer | |
| Date received | |

| | |
|---|---|
| Recommended action(s) | ☐ Seek further information / explanation from Client<br>☐ Escalate matter to senior management<br>☐ File an STR with any applicable regulator<br>☐ Sever relations with Client |
| Basis for recommended action(s) | |
| Signature of Compliance Officer | |
| Part 5: Follow-Up by Senior Management (If and Where Applicable) | |
| Recommended action(s) | |
| | ☐ File an STR with any applicable regulator<br>☐ Sever relations with Client<br>☐ Continue relations with Client |
| Basis for recommended action(s) | |
| Signature of member of senior management | |
| Date of recommendation(s) | |

## Appendix 6

## COMPLIANCE ACKNOWLEDGEMENT FORM

I, the undersigned, hereby acknowledge that I have read and understood the provisions contained in this Policy, and that:

(a) I will ensure my strict compliance with the policies, procedures and principles set out in this Policy;

(b) in the event I am unsure of any provision in this Policy, I will seek clarifications from the CO or any other personnel or officer as the Company may designated from time to time; and

(c) I understand there will be adverse consequences on the Company or its Clients that may result in the event of my non-compliance with this Policy.

Name: _____

Designation: _____

Date: _____

## Appendix 7

## SANCTIONS SCREENING REFERENCE

**INTERNATIONAL LISTS**

1. OFAC Consolidated List
2. OFAC SDN List
3. UK HM Treasury Office of Financial Sanctions Implementation Consolidated List
4. UK Home Office List of Proscribed Terrorist Organisations