

AML & CFT Policy

1. INTRODUCTION

Money laundering and the financing of terrorism have been identified as risks to ICICB CHAIN LIMITED (the “Company”). Legislation derives from the European Union Anti-Money Laundering Directives. Individual guidance is provided by each jurisdiction where the Company operates, hence we are obliged to adhere to this guidance. Gibraltar, as well as many other countries around the world, have passed legislation designed to prevent money laundering and to combat terrorism. This legislation, together with regulations, rules and industry guidance/codes, forms that cornerstone of Anti-Money Laundering (AML)/Countering the Financing of Terrorism (CFT) obligations for relevant financial businesses and outlines the offences and penalties for failing to comply. In particular, the Proceeds of Crime Act was amended on 16th March 2018 to bring within scope of AML “undertakings that receive, whether on their own account or on behalf of another person, proceeds in any form from the sale of tokenised digital assets involving the use of distributed ledger technology or a similar means of recording a digital representation of an asset.” The requirements of the different legislations apply to the Company globally. The Company may have additional local policies and procedures designed to comply with their local legislation, regulations and any government approved guidance in the jurisdiction(s) in which they operate.

2 POLICY STATEMENT

The Company and its directors are committed to full compliance with all applicable laws and regulations regarding money laundering and the financing of terrorism. Every officer, director, employee and associated person of the Company is responsible for assisting in the Company's efforts to detect, deter and prevent money laundering and other activities intended to facilitate the funding of terrorism or criminal activities through its business.

3. SCOPE

This Policy applies to all of the Company’s customers. This Policy also applies to all staff and any third party the Company might do business with.

4. LEGAL AND REGULATORY FRAMEWORK

The principal requirements, obligations and penalties, on which the Company's Systems and Controls are based, are contained in: • the EU Anti Money Laundering Directives; • the Proceeds of Crime Act 2015 in Gibraltar (the "Act", which transposes the EU Anti-Money Laundering Directive into Gibraltar law); • the Counter Terrorism Act 2010 in Gibraltar; • the Terrorism Act 2005 in Gibraltar; and • the Crimes Act 2011 in Gibraltar.

5. WHAT IS MONEY LAUNDERING

Money laundering is the generic term used to describe the process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source.

6. MONEY LAUNDERING OFFENCES & PENALTIES

6.1 Arrangements A person commits an offence if he enters into or becomes concerned in an arrangement which he knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person. The maximum penalty for this offence on conviction on indictment is fourteen years in prison or a fine or both. 6.2 Acquisition, possession or use of criminal property A person commits an offence if he- (a) acquires criminal property; (b) uses criminal property; or (c) has possession of criminal property. The maximum penalty for this offence on conviction on indictment is fourteen years in prison or a fine or both. 6.3 Concealing, transferring etc. proceeds of criminal conduct. A person commits an offence if he- (a) conceals criminal property; (b) disguises criminal property; (c) converts criminal property; (d) transfers criminal property; or (e) removes criminal property from Gibraltar. The maximum penalty for this offence on conviction on indictment is fourteen years in prison or a fine or both. 6.4 Tipping-off A person is guilty of an offence if- (a) he discloses that a money laundering suspicion report has been made or is being contemplated or is being carried out; and (b) the information on which the disclosure is based came to him in the course of a business or activity in the regulated sector The maximum penalty for this offence on conviction on indictment is five years in prison or a fine or both. 6.5 Failure to disclose: relevant financial business A

person is guilty of an offence if– (a) he knows, suspects or has reasonable grounds to suspect that another person is engaged in money laundering, or is attempting to launder money; (b) the information or other matter, on which that knowledge or suspicion is based came to his attention in the course of his trade, profession, business or employment; and (c) he does not disclose the information or other matter to the Gibraltar Financial Intelligence Unit (“GFIU”) as soon as is reasonably practicable after it comes to his attention. The maximum penalty for this offence on conviction on indictment is fourteen years in prison or a fine or both. TYPE: REGULATORY In addition to the criminal offences and consequences described above, there are also regulatory consequences the Company can face, such as: • Warning; • Licence suspension and/or revocation; • Personal management licence review and/or suspension/revocation; and • Financial penalties i.e.: fines.

7. WHAT IS TERRORISM FINANCING

Terrorist financing means (in accordance with Part 2.(1) of the Counter-Terrorism Act 2010 in Gibraltar, similar definition applies in the UK): (a) the use of funds or other assets, or the making available of funds or assets, by any means, directly or indirectly for the purposes of terrorism; or (b) the acquisition, possession, concealment, conversion or transfer of funds that are (directly or indirectly) to be used or made available for those purposes. Compared with money laundering (which involves the proceeds of all crimes), the amount of money that could be used as terrorism financing is quite small and can also come from legitimate sources. However, the social, political and economic consequences of allowing terrorist organisations to function and prosper are devastating and it is for this reason that Company staff must be on the alert for terrorist financing as well as for the proceeds of crime.

A person commits an offence if he- (a) Raises funds for terrorism (b) Uses and possesses money or other property for terrorism (c) Arranges funds for terrorism (d) Arranges the retention or control of terrorism property The penalty for these offences is fourteen years in prison or a fine or both.

8. TERRORISM FINANCING OFFENCES & PENALTIES

A person commits an offence if he- (a) Raises funds for terrorism (b) Uses and possesses money or other property for terrorism (c) Arranges funds for terrorism (d) Arranges the retention or control of terrorism property The penalty for these offences is fourteen years in prison or a fine or both.

9. MONEY LAUNDERING REPORTING OFFICER (MLRO)

It is a requirement for a director of the Company to have overall responsibility and oversight of all compliance matters by the Company and its officers and staff. The holder of this position, in the Company, would be a member of the board of directors. This position is known as the Compliance Officer. It is a requirement for the Company to appoint an MLRO. The holder of this position, in the Company, would be a member of the Compliance & Regulatory Team (if any, and failing that, an independent officer of the Company nominated by the Company's board of directors). This position is also known as the 'appropriate person' or 'nominated officer'. The MLRO is responsible for:

- Developing, implementing and overseeing all AML matters within the business;
- Undertaking a risk assessment for the business;
- Creating relevant policies, processes and procedures to prevent the Company from being misused for criminal activity;
- Providing training to staff in order for them to be able to identify red flags;
- Receiving and considering any internal suspicious activity reports;
- Liaising with the relevant Commissioner, the appropriate Financial Intelligence Unit ('FIU') and any other relevant government authority;
- Submitting regulatory reports; and
- Presenting an MLRO report to the Board, at least, annually whereby the operation and effectiveness of the Company's systems and controls is evaluated.

10. REPORTING: SUSPICIOUS ACTIVITY REPORTS (SAR)

The Company is required to report all circumstances where it has knowledge, suspicion or reasonable grounds to suspect that money laundering or the financing of terrorism is being or has taken place or attempted through its facilities. Employees are trained in order to recognise suspicious activities and therefore submit SARs where relevant. An internal SARs form is available on the Intranet for employees to use (please refer to Annex 1). The MLRO will also make the SARs form available to any employee upon request. The MLRO is responsible for investigating any internal SAR received and/or any suspicion of money laundering/ terrorist finance. The MLRO will acknowledge receipt of any internal SAR received. When considering a SAR, the MLRO will determine whether or not it needs to be disclosed to the authorities. This includes events in Gibraltar that may also be reported to other regulators and agencies. In making a decision, the MLRO will consider, amongst others:

- the information available regarding the case, i.e.: customer information, documentation, media news;
- transactions involved;
- account activity inconsistent with the customer's risk profile;
- correspondence with the customer;
- the reasons for

suspicion, etc. Based on the above consideration, if the MLRO knows or suspect or has reasonable grounds to know or suspect that money laundering or terrorist financing has taken place, then a disclosure will be made accordingly. In the case the MLRO decides not to make a disclosure, this will be thoroughly documented with the reasons why. Any disclosure is made to the appropriate country FIU, which in Gibraltar is the GFIU. 10.1. SAR's Log The MLRO will record all internal SARs received by employees in the SAR's Log. This Log will be kept up to date with any new information that might arise on any given case.

11. AML/CFT RISK ASSESSMENT

The Company shall perform a risk assessment, at least, on an annual basis. There will be triggers and thresholds in place as part of the assessment. The risk assessment will be conducted on all customers. The customer's risk profile will be reviewed at least annually and/or where there is a trigger event which prompts the review. If and when necessary, the Company will implement remediation projects in order to deal with any deficiencies which might be identified as part of the Know Your Customer/Customer Due Diligence process. Based on this risk assessment, the level of due diligence will vary, as set out in section 12 below, taking into consideration the following type of risks:

11.1. Customer Risk This is the identification of the risk posed by the type of customer: • politically exposed persons; • high rollers (high spender); • customer whose spend isn't consistent with their wealth or income; and • customer located/residing in a high risk jurisdiction.

11.2 Customer profile Each customer will have a risk profile based on factors such as: • payment method, i.e. deposit via one method and withdrawal via another; • using high risk payment methods, i.e. prepaid cards, cryptocurrencies, etc.; • account activity, i.e. significant changes in customer account activity; • products used, i.e. cryptocurrencies, tokens, etc.; • balance, i.e. amount of deposits and value, withdrawal practices, etc.; • Any other risk factor identified as part of the onboarding risk assessment process and/or ongoing business relationship, i.e. money laundering and/or terrorist financing risks.

11.3. Product Risk This is the type of product(s) offered by the Company including, the company's tokens and access to the Company's platform.

11.4. Interface Risk The Company recognises that, as a seller of tokens, it will never meet its customers face to face. Therefore, the interface risk is already considered high.

11.5. Country Risk Country risk is used to describe the risk posed to the Company by the geographic origin of the economic activity of the business relationship. This is wider than just the country of residence of the customer and will, for example, include where the customer's money is coming from. The Company will determine which countries are high risk based on the High-risk and non-cooperative jurisdictions list produced by the Financial Action Task Force as well as the Corruption Perception Index from Transparency International.

12. CUSTOMER IDENTIFICATION (KNOW YOUR CUSTOMER) AND CUSTOMER DUE DILIGENCE

12.1 The Act The Act transposes the EU Anti-Money Laundering Directive into Gibraltar law. The Act sets out that a 'relevant financial business' must apply different levels of due diligence measures based on a risk based approach, and these are either: (a) Customer due diligence ("CDD"); (b) Simplified due diligence ("SDD"); or (c) Enhanced due diligence ("EDD").

12.1.1 Customer Due Diligence Policy (CDD) Section 11 of the Act states that a 'relevant financial business' must apply customer due diligence measures where it does any of the following: (a) establishes a business relationship; (b) carries out an occasional transaction amounting to €15,000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked; (c) in the case of persons trading in goods, when carrying out occasional transactions in cash amounting to €10,000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked; (d) suspects money laundering or terrorist financing, regardless of any derogation, exemption or threshold; (e) doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification; (f) constitutes a transfer of funds, as defined in Article 3(9) of Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (1), exceeding €1,000. (g) for providers of gambling services, upon the collection of winnings, the wagering of a stake, or both, when carrying out transactions amounting to 2,000 euro or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked. It is a requirement under section 12 of the Act that a 'relevant financial business' must conduct an ongoing monitoring of the business relationship, which means that the entity must scrutinize transactions undertaken throughout the course of the business relationship in order to ensure that such transactions are consistent with: (a) the relevant financial business's or person's knowledge of the customer; (b) their business and risk profile. Where an entity seeks to establish a business relationship or carry out a transaction amounting to €15,000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked and is carrying out due diligence measures, the entity must verify the identity of the customer before the establishment of a business relationship or the carrying out of an occasional transaction. CDD is required by law since you can better identify suspicious transactions if you know your customer and understand the reasoning behind their dealings with you. CDD involves a combination of SDD and EDD as further explained below.

12.1.2 Know Your Customer ("KYC") KYC is the process used by the Company to verify the identity of our customers. There are different levels of due diligence we need to perform. This will be determined on a risk based approach. The Company will apply CDD when: (a) it establishes a business relationship; (b) it suspects money laundering or terrorist financing; (c) it doubts the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification; and (d) it receives any amounts from the sale of tokens. Moreover, the Company will also apply CDD: (e) in relation to any transaction¹ that amounts to €150 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked; (f) at other appropriate times to existing customers on a

risk-based approach; (g) when the Company becomes aware that the circumstances of an existing customer relevant to its risk assessment for that customer have changed; or where there is a legal duty to contact the customer (in the case of a customer that is not an individual) for the purpose of reviewing any information relating to the beneficial owner or beneficial owners 12.1.3. Enhanced Due Diligence (EDD) A 'relevant financial business' must apply EDD measures to appropriately manage and mitigate risks: (a) in the cases referred to in Articles 19 to 24 of the European Union Fourth Anti-Money Laundering Directive (the "Directive"); (b) when dealing with natural persons or legal entities established in third countries identified by the European Commission as high risk third countries; and (c) in other cases of higher risk identified: (i) by the relevant financial business; or (ii) by the Minister by notice in the Gazette. EDD measures need not be invoked automatically with respect to branches or majority-owned subsidiaries of obliged entities established in the European Union which are located in high-risk third countries, where those branches or majority-owned subsidiaries fully comply with the group-wide policies and procedures in accordance with Article 45 of the Directive, and such cases must be handled on a risk sensitive basis. Where the customer is not physically present for identification purposes, the relevant entity must take specific and adequate measures for the higher risk, such as: (a) ensuring that the customer's identity is established by additional documents, data or information; (b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution which is subject to the Directive; and (c) ensuring that the first payment is carried out through an account opened in the customer's name with a credit institution. The Company will apply enhanced customer due diligence measures and enhanced ongoing monitoring in order to manage and mitigate the money laundering or terrorist financing risks arising in the following cases: (a) where there is a high risk of money laundering or terrorist financing; (b) where the customer is situated in a high-risk third country identified by the European Commission or by the FATF (whichever has the lower threshold); (c) where a customer or potential customer is a PEP, or a family member or known close associate of a PEP; (d) in any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, and the transaction or transactions have no apparent economic or legal purpose; (e) for VIP customers; and 1 'Transaction' consists of: (f) The sale of ICICB Coins. (g) in any other case which, by its nature, can present a higher risk of money laundering or terrorist financing. Before a customer is considered a VIP, additional checks will be performed in order to be satisfied with the information we hold for the customer, i.e. level of expending in line with income, etc. Where the Company discovers that a customer has provided false or stolen identification documentation or information, and/or where the information held by the Company differs from that of the customer's transaction patterns, the relationship will be terminated. Any customer account closed on these circumstances, will be added to an internal blacklist. The enhanced measures will include, but not be limited to: (a) examining the background and purpose of the transaction, as far as reasonably possible; (b) increasing the degree and nature of monitoring of the business relationship in which the transaction is made, to determine whether the transaction or the relationship appear to be suspicious; (c) depending on the requirements of the case, may also include, among other things: ü seeking additional independent, reliable sources to verify information provided or made available to the Company; ü taking additional measures to understand better the background, ownership and financial situation of the customer, and other parties to the transaction, i.e. payslips, savings, inheritance, bank statements, etc.; (d) taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship; (e) increasing the monitoring of the business relationship, including greater scrutiny of the transactions. Section 17(6) of the Act prescribes in relation to business relationships or transactions involving high-risk third countries specifically, that a relevant financial business must apply

the following EDD measures: (a) obtain additional information on the customer and on the beneficial owners; (b) obtain additional information on the intended nature of the business relationship; (c) obtain information on the source of funds and source of wealth of the customer and of the beneficial owners; (d) obtain information on the reasons for the intended or performed transactions; (e) obtain the approval of senior management for establishing or continuing the business relationship; and (f) conduct enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination. Therefore, applying CDD measures involves several steps: 1. The Company is required to identify customers; (a) identification of a customer means being told or coming to know of the customer's identifying details, such as their name and address. The Company identifies the customer by obtaining a range of information about the customer. 2. The Company must then verify the customers identities, upon registration; (a) verification means obtaining some evidence which supports this claim of identity. The verification of the identity consists of the Company verifying the information received against documents, data or information obtained from a reliable and independent source. 3. The Company must also verify and whitelist the wallets from which customers remit any cryptocurrencies; (a) verification means obtaining some evidence which confirms the wallet: (i) is not related to terrorist financing; (ii) is not related to the darknet market; (iii) does not belong to mixers; or (iv) does not relate to a sanctioned country. The verification of the wallet consists of the Company verifying the information received against documents, data or information obtained from a reliable and independent source. 4. The company shall also collect IP addresses and to the extent applicable MAC addresses from its customers during the identification and verification process.

Simplified Due Diligence (SDD) The Act states that where a 'relevant financial business': (a) identifies areas of lower risk; and (b) has ascertained that the business relationship or the transaction presents a lower degree of risk; it may, in accordance with section 16 of the Act apply simplified customer due diligence measures. Section 16 of the Act should not be construed as derogating from the need to undertake sufficient monitoring of the transactions and business relationships to enable the detection of unusual or suspicious transactions or from the provisions of section 12 of the Act. When assessing the risks of money laundering and terrorist financing relating to types of customers, geographic areas, and particular products, services, transactions or delivery channels, a relevant financial entity must take into account at least the factors of potentially lower risk situations set out in Schedule 6 of the Act.

12.2 Gibraltar Specifics

12.2.1 Customer Due Diligence (CDD) CDD is a two stage process which will always be undertaken upon registration. It consists of: 1. first, the operator must obtain the required personal identification details through an effective and reliable customer registration process; and 2. thereafter verify that identity using reliable and independent means, including databases, documents or other supplementary methods of confirming/assuring identity.

12.2.2 Enhanced Due Diligence (EDD) All customers that make a deposit will be subject to EDD. This will consist of CDD plus an additional third stage that includes: (a) undertaking additional information checks; or (b) supplementary measures to verify or certify documents; or (c) ensuring that payments from or to the customer are from/to a bank account or cryptocurrency wallet in his name. The above measures would be in addition to the arrangements to establish identity or age and will be recorded. EDD will be performed as soon as practicable: (a) where a customer makes the first deposit in fiat currency or cryptocurrency; (b) where a customer's deposits reach the equivalent of €150 (or equivalent); and (c) where a customer seeks to withdraw fiat currency or cryptocurrency; In any case, where EDD is necessary, additional information and/or documentation will be requested, i.e. source of wealth, source of funds, payment method ownership, etc. Additional verification is also performed. If the EDD process is not concluded in a reasonable timeframe (generally within 28 days), the account will be

subject to additional and proportionate supervision, consistent with the value and risk profile of the account and the deposits. Where the verification process fails then no further transactions will be allowed, including transfers or withdrawals in fiat currency or cryptocurrency. Where necessary, deposits in fiat currency or cryptocurrency will be retained until identification is resolved. Therefore, CDD is a three stage process: 1) obtaining sufficient information on customer identity; 2) verification of that identity against reliable and independent means; and 3) further identity verification by way of additional database checks, "supplementary means" or a bank process or cryptocurrency wallet whitelisting process in the name of the customer. Policy Section 2(1) of the Act states: "A person commits an offence if he enters into or becomes concerned in an arrangement which he knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person." Section 8 of the Act states that "business relationship" means: "a business, professional or commercial relationship which is connected with the professional activities of a relevant financial business and which is expected, at the time when contact is established, to have an element of duration." Section 9(1)(p) of the Act brings companies which carry out token sales within the definition of "relevant financial business" as follows: "(p) undertakings that receive, whether on their own account or on behalf of another person, proceeds in any form from the sale of tokenised digital assets involving the use of distributed ledger technology or a similar means of recording a digital representation of an asset." By virtue of the fact that it will carry out its sale of tokens from Gibraltar, the Company will need to ensure compliance with the Act and apply appropriate customer due diligence measures to all the participants in the Company's token sale. The directors and officers of the Company are notified of the overarching responsibility imposed by Section 2(1) of the Act which creates an offence if a person enters into or becomes concerned in an arrangement which he/she knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person. In light of this, the following KYC procedures have been adopted by the Company:

12.2.3 Individual Participants

(a) Information to be received from any individual participant in the Company's token sale who pays an amount less than €150 (or currency equivalent): (i) full legal name; (ii) usual residential address; (iii) date of birth; (iv) verification of email address; (v) wallet address; and (vi) IP address and to the extent applicable a MAC address.

(b) Additional documentation to be received from each individual participant in the Company's token sale who pays between €150 and €10,000 (or currency equivalent): (i) passport copy; and (ii) a second recognised form of photographic identification.

(c) Additional documentation to be received from each individual participant in the Company's token sale who pays between €10,000 and €50,000 (or currency equivalent) and is considered a low risk participant: (i) passport copy; (ii) a second recognised form of photographic identification; and (iii) plausible and verifiable source of wealth.

(d) Additional documentation to be received from each individual participant in the Company's token sale who pays over €150 (or currency equivalent) and is considered a high risk participant: (i) passport copy; (ii) a second recognised form of photographic identification; and (iii) documentary and verifiable proof of source of wealth.

(e) Additional documentation to be received from each individual participant in the Company's token sale who pays more than €50,000 (or currency equivalent): (i) passport copy; (ii) a second recognised form of photographic identification; and (iii) documentary and verifiable proof of source of wealth. Notwithstanding the above, where the business relationship or transaction involves an individual from a high-risk third country, the Company will request any information and documentation, not already obtained in accordance with the above procedure, that is necessary to comply with Section 17(6) of the Act.

12.2.4. Due Diligence for Corporate Participants

Information and documentation to be received from any corporate participant in the

Company's token sale: (i) certificate of incorporation of the corporate entity; (ii) memorandum and articles of association of the corporate entity; (iii) register, or certificate from the corporate registry, showing all the directors and shareholders of the corporate entity; (iv) if the corporate entity is over 12 months old, a certificate of good standing for the corporate entity; (v) if the shareholder (or any of the directors of the shareholder) up to each ultimate beneficial owner, is a corporate entity, the documents listed (i)-(iv) above for each corporate shareholder and corporate director in the structure; (vi) the documents listed in the "Individual Participants" section relating to the ultimate beneficial owner(s) of the corporate participant, in accordance with their risk profile; (vii) verification of e-mail address of each corporate entity, (viii) verification of IP address of each corporate entity; (ix) verification of cryptocurrency address that will be used to make a payment; and (x) email for contact person (person who has responsibility to contact us); The principal requirement is to look behind a corporate entity to identify the individuals who control the entity and its assets, with particular attention being paid to any shareholders or others who exercise a significant influence over the affairs of the company. For companies with multi-layered ownership structures, the company is required to document their understanding of the ownership and control structure of the natural and legal persons at each stage in the structure. This does not require for director and shareholder information to be obtained at every level, but documentation should be obtained from reliable and verifiable sources that confirm the company's existence, its registered shareholdings and management. Confirmation of identity is required for any individuals who own more than a 25% share in the company with whom the business relationship is being established. Notwithstanding the above, where the business relationship or transaction involves a corporate entity from a high risk third country, the Company will request any information and documentation, not already obtained in accordance with the above procedure, that is necessary to comply with Section 17(6) of the.

13. ANONYMOUS AND/OR DUPLICATE/MULTIPLE ACCOUNTS

The Company does not permit the use of anonymous and/or duplicate/multiple accounts. The Company has the necessary systems and controls in place to detect and deter these occurrences. If a customer is found to have opened more than one account, the accounts will be closed. The Company will use a software (or procure the services of a third-party service provider) to be able to identify this type of accounts. Daily reports will then be analysed by the Risk and Payment Team, who will then take actions (i.e.: close accounts) accordingly.

14. ONGOING MONITORING

The Company performs ongoing monitoring of its customers. The Company uses a software provider who analyses customers' historical information and account profile. This is the way a "whole picture" is produced which analysis customer's profile, risk levels, and predicted future activity. The software also generates reports and create alerts to suspicious activity which are further analysed by the Company in order to take actions accordingly. There will also be instances whereby the analysis of transactions, information and/or documentation needs to be done manually. The responsibility for this analysis will depend on various factors, but generally will be performed by fraud, risk and/or compliance.

14.1. Type of Monitoring Based on a variety of internal reports, including exception reports, the Company will carry out the following monitoring:

14.1.1 Product monitoring Monitoring of products used by customers, in order to identify changes/irregular patterns/behaviour.

14.1.2. Transaction and activity monitoring This will include but not be limited to:

- change of payment methods;
- whether the transactions or activity are inconsistent (unusual) with the customer's risk profile;
- whether the transactions or activity are complex or unusually large;
- whether the transactions or activity form part of an unusual pattern;
- whether the transactions present a higher risk of money laundering or financing of terrorism; or
- change in customer behaviour.

14.1.3. Media monitoring This will monitor news media on specific countries, languages and publications. The Company will use a software provider to monitor media. The information will be analysed by Compliance (if any, and failing that, by the board of directors).

15. RECORD KEEPING

The Company keeps records of the procedures applied to establish the identity of its customers, and records of the value of their transactions, for at least 5 years after the relationship ends. This is consistent with data protection legislation and AML/CFT requirements. GDPR matters are covered in section 23 of this Manual.

16. POLITICALLY EXPOSED PERSONS ("PEPs")

A PEP generally presents a higher risk for potential involvement in bribery and corruption by virtue of their position and the influence that they may hold.

16.1. Definition The Directive defines a 'politically exposed person' as a natural person who is or who has been entrusted with prominent public functions and includes the following: (a) heads of State, heads of government, ministers and deputy or assistant

ministers; (b) members of parliament or of similar legislative bodies; (c) members of the governing bodies of political parties; (d) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances; (e) members of courts of auditors or of the boards of central banks; (f) ambassadors, chargés d'affaires and high-ranking officers in the armed forces; (g) members of the administrative, management or supervisory bodies of State-owned enterprises; (h) directors, deputy directors and members of the board or equivalent function of an international organisation. No public function referred to in points (a) to (h) shall be understood as covering middle-ranking or more junior officials; 'family members' includes the following: (a) the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; (b) the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person; (c) the parents of a politically exposed person; 'persons known to be close associates' means: (a) natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person; (b) natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person. All identified PEPs will be assessed by senior management and a decision will be made on whether to continue with the relationship or terminate it. This will then be recorded in the PEPs Log.

PEPs are monitored on a daily basis, using a data software, in order to identify any new information which might change their risk profile

17. SANCTION LISTS

All new customers are screened against sanction lists. If a potential or current customer is identified as being in a sanction list, the relationship will be terminated immediately. Under no circumstances the Company will, knowingly, engage in a relationship with a person and/or organisation appearing in a Sanctions List. Screening of customers against PEPs databases and Sanctions Lists is performed on a daily basis

18. COOPERATION WITH GOVERNMENT BODIES

The Company is committed to the fight against money laundering and the financing of terrorism. As such, the Company will cooperate with any and all law enforcement requests and/or investigations, the GFIU, the Royal Gibraltar Police and any other relevant government authority. 18.1. External Data

Request Any external request received by the Company will be dealt with by the Compliance Department (if any, and failing that, by the board of directors) or other officer and escalated to a director where appropriate. All staff is made aware of this process, both, through this Policy and via internal email communications.

19. COMMUNICATION

This policy will be placed on the Intranet page and also communicated to staff by email. When the Company engages in business with third parties, this Policy will be provided. Any changes or amendments to this Policy, will also be communicated to relevant stakeholders (i.e.: employees, third parties, etc.) accordingly.

20. REVIEW

The Company will review this policy, at least, every year. The review will involve all relevant stakeholders. The Company will make such changes as are reasonably necessary to comply with this Policy and any ongoing license obligations.

21. NON-COMPLIANCE

All Company's employees are required to read and comply with this policy. Failure to comply with this policy would be considered gross misconduct and might result in termination of employment.

22. STATEMENT ON OUTSOURCING

22.1 Responsible Persons

22.1 Responsible Persons The persons responsible are members of the Board of Directors and non-Board Members who offer or execute a service on behalf of and under the direction of the Board of Directors, inclusive of persons who are employees of an outsourced service provider. 22.2 Scope (a) This policy is intended to be used as the basis for all circumstances in which the Company elects to outsource functions and activities. (b) Its purpose is to ensure that all outsourcing undertaken will: i. Support the

Company's business strategy and key objectives. ii. Provide customers with an experience at least as good, or better than an in-house alternative. iii. Enable the Company to deliver a service experience to customers at a cost consistent with the Company's cost objective/budget/business plan. iv. Enable the Company to exercise control over outsourced service providers to ensure that any risks are properly identified, understood and appropriately mitigated. v. Enable the Company to demonstrate as required that its responsibilities in respect of outsourced activities are being effectively discharged. 22.3 Application of guiding principles A risk-based approach will be adopted which will determine the level of supervision and control to each outsourced activity. 22.4 Outsourcing Responsibility (a) Given the importance of outsourcing to the Company's business operations all outsourced activities critical to the successful delivery of customer experience will be subject to Board approval. (b) Ultimate responsibility lies with the Board of Directors. (c) It will also be the responsibility of the Board to ensure that the regulator (if required) is appropriately informed in the event that material activities are to be outsourced. 22.5 KYC/AML All outsourced service providers will be subjected to the Company's KYC/AML process that will ensure they have: (a) The Ability; (b) The Capacity; (c) The Financial Capability; (d) And the authorization required by law and/or regulation to undertake the activities to be outsourced on a professional, efficient and effective basis meeting the standards prescribed by the Company. 22.6 Contractual Arrangements (a) All outsourced arrangements will be the subject of written contracts which will comprise a legal agreement and accompanying services and service levels. (b) It is advisable that agreements include the following: i. Definition of the activities to be outsourced: ii. Responsibilities of the Company and the outsourced service provider: iii. Defined intellectual property and client ownership and protection of confidential information including ownership/use of records: iv. Ensure that the Company is able to meet its legal obligations: v. Obligation on the service provider to allow the Company and Company's external auditors to relevant data and premises as required and to allow the Company and Company's external auditors full and unrestricted rights of inspection and audit of service provider data: vi. Provision of continuous monitoring and assessment of services provided: vii. Provision of necessary conditions for any sub-contracting by the service provider which will include any need for approval from the Company and ensure that the Company maintains control over all sub-contracted activity: viii. Obligation on service provider to immediately inform the Company of any changes in circumstances which may materially impact on the delivery of outsourced services: ix. Obligation on services provider to notify the Company of potential or actual conflicts of interest: x. Agreed renewal, termination and exit management processes that ensure there is no customer detriment: xi. Definitions of material breach and consequences of same: xii. Extent of liability, quantum attaching to the Company and to outsourced service provider and circumstances under which liability may materialize: xiii. Choice of law where the service provider is located outside of Gibraltar: xiv. General Data Protection Requirements of service provider: xv. Stipulation of any required guarantees and indemnitees from service provider: xvi. Agreed dispute resolution procedure: xvii. Payments processes: xviii. Requirement for appropriate indemnity or other insurance to be held by the outsourced service provider: xix. Minimum reporting standards from the outsourced service provider to the Company specifying content and timing: xx. Specific complaints handling processes, procedures, referral and reporting requirements: xxi. Agreed rectification actions where performance shortfalls are noted. 22.7 Contingency Planning (a) The Company's business continuity and disaster recovery plans will include provision for all outsourcing activities: (b) Planning in connection with the activities of each outsourced service provider shall be undertaken in conjunction with that service provider: (c) The Company's business continuity and disaster recovery plans will include provision for the need to quickly transfer outsourced activities either to

another branch of the service provider or another outsourced service provider: (d) Requirement of copy of business continuity and disaster recovery plan to be lodged with the Company and any test results and subsequent changes notified to the Company. 22.8 Termination and Exit Management Contracts between the Company and outsourced service providers must adequately define the agreed termination and exit process including: (a) Minimum notice period (termination without cause): (b) Ability to terminate with cause: (c) Termination should also include provision to allow the Company to terminate by notice of dismissal or extraordinary notice of cancellation if required: (d) Exit strategies should allow transfer of service to another outsourced service provider or the Company to ensure continuity of the service and return of customer data and other property and resources of the Company: (e) The Company to have the right to require the co-operation of the service provider in the event of termination that will enable the Company to bring the function in-house or an orderly transfer to an alternative service provider

23. GENERAL DATA PROTECTION REGULATIONS (“GDPR”)

This Privacy Notice explains how and why the Company may use personal data, The handling of personal data is treated seriously and the Company respects privacy and rights to control personal data. 23.1 How the Company collects data The Company collects personal data when an individual registers their personal details directly with the Company in respect of the proposed token sale. 23.2 Lawful basis on which Personal data is relied upon (a) Where an individual has actively registered their interest through the Company’s website, the lawful basis for holding and processing personal data would be a “contractual” basis. (b) Personal data collected is subject to third party checks as part of the token sale requirement to combat Money Laundering. In these circumstances where there is a direct contractual relationship between the Company and the individual, the Company is collecting and processing personal data on the basis of legitimate interest. By providing personal data for this purpose individuals accept and agree that the basis upon which the Company is processing personal data is legitimate interest. The Company will only process personal data in accordance with the GDPR. (c) The Company would also retain and process personal data if there is a legal obligation to do so. In order to operate and improve our business, there is also a valid legitimate interest basis for holding and processing of personal data. The Company might also have requested explicit consent in order to use personal data. Where the Company processes personal data based on consent, individuals have a right to withdraw consent at any time. 23.3 Principles for collection and processing of personal data The Company has adopted the following general GDPR principles to support and govern its collection and processing of Personal Data: • Personal Data shall be processed lawfully, fairly, and in a transparent manner. • Personal Data shall only be retained for as long as it is required to fulfil contractual requirements. • Personal Data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are collected and/or processed. • Personal Data shall be accurate and, where necessary, kept up to date. • The Data Subject has the right to request from the Company access to and rectification or erasure of

their personal data, to object to or request restriction of processing concerning the data, or to the right to data portability.

23.4 Disclosure of Personal Data The Company may disclose personal data to certain permitted third parties, such as third-party service providers or cloud service providers, to comply with contractual obligations. The Company will never sell personal data and will only share it with organisations the Company works with when it's necessary and the privacy and security of personal data is assured.

23.5 Personal Data Retention Policy The Company will keep personal information for as long as the Company need it for the purpose it is being processed for, considering any legal obligation the Company may have (e.g. to maintain records for fiscal or reporting purposes), any other legal basis the Company may have for using information The Company will keep the information for a period as set by GDPR.

23.6 Data Subject Right Individuals have certain rights over their personal data and data controllers are responsible for fulfilling these rights. The Company are the data controllers, where we decide how and why personal data is processed. Under GDPR, individuals have a right to: (a) know what data is processed, how it is processed and shared and to receive a copy of their personal data (b) erasure, where there are no laws or regulations which mandate the retention of that data (c) rectification of inaccurate personal data (d) withdraw their consent (e) data portability (f) restriction of processing of specific personal data items (g) object to processing performed in the legitimate interests of the Company subject with the objection evaluated in the context of the risk to the data subject (h) object to direct marketing and have the direct marketing ceased immediately (i) be subject to a decision based solely on automated processing (j) claim compensation for damages caused by a breach of the Act

23.7 Access to Personal Data An individual's right to access can be exercised in accordance with the EU General Data Protection Regulation 2016. Any requests from data subjects about the information held on them must be documented and include the nature of the request and the response given. To progress your request two forms of identification (ID) will also be required before any data is compiled, these must be dated within the last three months. The Company, upon being satisfied that an individual meets the criteria for disclosure of data under GDPR, will provide a response to the individual within 28 days from that date.