Anti-Money Laundering Policy

CF Technologies Ltd – C87860 – Centris Business Gateway, Level 4/W,
Triq Is-Salib Tal-Imriehel, Central Business District, Zone 3, Birkirkara, CBD3020, Malta.

INDEX

1. INTRODUCTION

1.1 This Anti-Money Laundering Policy is established, and may be amended by, the Board of Directors.

1.2 The meaning of certain capitalized or uncapitalized terms used in this AML Policy is set forth in the List of Definitions attached as **Annex 1**.

2. APPLICATION

2.1 The Anti-Money Laundering Policy ("**AML Policy**") applies to XCOINS ("**Company**") and their directors, officers, full-time, part-time and seconded employees, and anyone working on XCOINS behalf, e.g. consultants and representatives. Personnel are expected to act in a manner that will enhance XCOINS reputation for honesty, integrity and reliability. The AML Policy applies in all countries in which XCOINS operates or conducts business. When the laws of those countries require a higher standard, the local standard will take precedent. Adherence to this AML Policy is a condition of employment and/or engagement with the Company, and therefore the Employees must acknowledge on an annual basis that they have understood the AML Policy and have disclosed any suspected and actual violations through appropriate channels.

2.2 The AML Policy will not give answers for every ethical or legal situation. If Employees have any doubts about the right thing to do, they should seek advice from the MLRO.

2.3 If Employees violate XCOINS policies and procedures or any of the laws that govern XCOINS business, XCOINS will take immediate and appropriate action up to and including termination of employment.

2.4 The purpose of this AML Policy is to substantially prevent, manage and mitigate the risk that XCOINS and their Employees become directly or indirectly involved in actual or potential money laundering activities, or terrorist financing activities.

2.5 This AML Policy sets out the key principles and obligations in relation to the AML Framework in order to identify and assess the Money Laundering ("**ML**")/Terrorism Financing ("**TF**") risks to which XCOINS is exposed to ("**ML/TF**", respectively the "**AML**" measures, or more broadly "AML"), as defined below.

2.6 For the purpose of this AML Policy, a counterparty comprises of: XCOINS shareholders, customers, Employees, financial institutions, service providers and

any business relationship. A 'business relationship' means a business, professional or commercial relationship which is connected with the professional activities of the institutions and persons covered by such law and which is expected, at the time when the contact is established, to have an element of duration.

3. GOVERNANCE

3.1 The Board of Directors are ultimately responsible for monitoring and enforcing compliance with the AML Policy andhave the final responsibility for developing and executing mitigation actions in case of issues. This is set out in more detail in the Governance Framework.

3.2 The Board of Directors are ultimately responsible for compliance with all relevant laws, regulations, rules and professional standards applicable to Xcoins, whereunder those with respect to AML. This is set out in more detail in the Governance Framework.

3.3 The Board of Directors are responsible for the day-to-day execution of the risk management function. This is set out in more detail in the Governance Framework.

4. DEFINITIONS OF MONEY LAUNDERING AND TERRORISM FINANCING

4.1 Money Laundering is the process by which it attempts to hide and disguise the true origin and ownership of the proceeds from criminal activities, thereby avoiding prosecution, conviction and confiscation of criminal funds.

4.2 Terrorism Financing means: the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any terrorist act.

5. OBLIGATIONS

5.1 The main obligations for XCOINS and its Personnel under this AML Policy are as follows:

- perform a risk assessment on overall activities, including contemplated activities;
- perform an individualized counterparty due diligence on a risk-sensitive basis; and
- report to and cooperate with the competent authorities (if required).

5.2 XCOINS complies with all applicable laws and regulations wherever XCOINS conducts business, enters into, or maintains business relationships.

6. RISK ASSESSMENT

6.1 XCOINS has adopted the AML Policy and has put procedures in place to mitigate the risk it may become directly or indirectly involved in actual or potential money laundering activities, or in terrorist financing activities.

6.2 XCOINS takes a risk-based approach to prevent, manage and mitigate AML offences, including (but not limited to):

- identification of the risk of AML to which it could be exposed;
- categorizing such risk in accordance with its internal risk categorization methodology; and
- defining and implementing appropriate measures to mitigate the identified risk.

6.3 In the risk-based approach, XCOINS takes into account the nature and the size of its activities and the risk factors related to:

- types of counterparties;
- types of (envisaged) products with the counterparties;
- types of (envisaged) services with the counterparties;
- the delivery channels;
- the countries and geographical locations of XCOINS operations.

Xcoins examines, as far as reasonably possible, the background and purpose of all complex and unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. XCOINS increases its degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear suspicious.

7. COUNTERPARTY DUE DILIGENCE ("CDD")

7.1 Consistent with a risk-based approach, XCOINS will, before the establishment of a business relationship or the carrying-out of a transaction, as part of all due diligence measures that are applied to such business relationship or transaction:

- identify and verify the identity of its counterparty
- assess the level of AML risk such counterparty could present; and
- decide the intensity (*i.e.* simplified, standard or enhanced) of the AML Counterparty Due Diligence it applies.

7.2 The due diligence measures performed are documented and kept on file.

7.3 The Board of Directors monitors the due diligence performed by responsible Employees and shall review the assessment performed and any supporting documentation, as relevant.

7.4 It is prohibited that accounts are kept under fictitious names.

7.5 "**Counterparty due diligence measures**" comprise, where applicable:

- identifying the counterparty and verifying the counterparty's identity based on documents, data or information obtained from reliable and independent sources; and

7.6 The following is a non-exhaustive list of risk variables that XCOINS considers when determining to what extent it shall apply counterparty due diligence measures:

- the purpose of the account or relationship;
- the (intended) regularity or duration of the business relationship;
- the risk profile; and
- the results of financial sanctions/Politically Exposed Person ("**PEP**")/negative media screening.

7.7 **Simplified Counterparty Due Diligence ("Simplified CDD")**

7.7.1 In case of low AML risk, XCOINS may opt to apply a Simplified CDD. The conclusion that simplified CDD is appropriate will always be based on a risk assessment. XCOINS can carry out a prior assessment of the cases in which simplified CDD will be used. This will be done by means of a prior risk analysis, taking into account the risk factors on the basis of which the low-risk counterparties will be identified. Factors of potentially lower AML risk situations areas are set out in Annex 3.

7.7.2 Simplified CDD consist of a verification of the declared identity of the counterparty against the relevant public register and/or other available sources, and assessing the information received on the purpose and intended nature of the business relationship.

7.8 Standard Counterparty Due Diligence ("Standard CDD")

7.8.1 Standard CDD is carried out by XCOINS when onboarding and entering into a business relationship and the carrying-out of a transaction its counterparties and there are no material factors of increased AML risks, as set out in Annex 2, found. Standard CDD consists of:

- identifying the counterparty with whom the business relationship is entered with;
- verifying the identity declared by the counterparty in the application form against documents, data or information from reliable and independent sources; and

7.9 Enhanced Counterparty Due Diligence ("Enhanced CDD")

7.9.1 Enhanced CDD will be applicable when an increased AML risk is identified. Factors of potentially increased AML risk situations are set out in Annex 2.

7.9.2 Enhanced CDD will also be applicable when dealing with natural persons established in third countries which do not or insufficiently apply AML measures.

8. MONITORING AND REPORTING

8.1 As part of the ongoing relationship with the counterparty, ongoing AML monitoring will be carried out on a risk-based approach and where needed or otherwise required. In case unusual transactions, such as data changes, payments or withdraws, or activities potentially linked to money laundering, are identified, further investigation will take place. Transactions / activities not consistent with the initially declared purpose or nature of the relationship may also be further investigated. This is set out into more detail in the Compliance Program.

8.2 All Employees will endeavor to avoid carrying out a transaction which they know or suspect or have reasonable grounds to suspect to be related to money laundering. Unusual transactions shall be escalated to the Board of Directors.

8.3 An internal log will be maintained by the MLRO with information on all unusual transactions escalated to theBoard of Directors, the investigations carried out for each report received and the outcome of such investigation, including whether the instance was reported to the authorities or not.

8.4 The MLRO will report to the Board of Directors, on an as needed basis, on unusual or suspicious transactions, their status and the outcome of investigations carried out.

9. COOPERATION WITH AUTHORITIES

9.1 All Employees are obliged to cooperate fully with the appropriate governmental authorities responsible for combating AML, if required. If needed, this could include reporting suspicious transactions and cooperating with the authorities, or inform promptly, on their
own initiative, the appropriate authority when they know, suspect or have reasonable grounds to suspect that money laundering, an associated predicate offence, or terrorist financing is being committed or has been committed or attempted, in particular in consideration of the person concerned, its development, the origin of the funds, the purpose, nature and procedure of the operation.

9.2 The identity of the Employees or authorized representatives having provided such information is kept confidential by the aforementioned authorities, unless disclosure is essential to ensure the regularity of legal proceedings or to establish proof of the facts forming the basis of these proceedings.

10. MISCELLANEOUS

10.1 **Occasional non-compliance**. Subject to applicable law and regulation, the Board of Directors may occasionally and in specific events decide at its sole discretion that this AML Policy can be deviated from.

10.2 **Amendment**. This AML Policy may be amended by the Board of Directors at its sole discretion without prior notification.

10.3 **Interpretation**. In case of uncertainty or difference of opinion on how a provision of this AML Policy should be interpreted, the opinion of the Chairman shall be decisive.

10.4 **Governing law and jurisdiction**. This AML Policy is governed by the laws of Malta. The courts of Malta have exclusive jurisdiction to settle any dispute arising from or in connection with this AML Policy (including any dispute regarding the existence, validity or termination of these rules).

10.5 **Complementarity to law and Articles of Association**. This AML Policy is complementary to the provisions governing the Board of Directors as contained in laws and regulations and the Articles of Association. Where this AML Policy is inconsistent with laws and regulations, the latter shall prevail. Where this Code is consistent with the Articles of Association but inconsistent with laws and regulations, the latter shall prevail.

10.6 **Partial invalidity**. If one or more provisions of this AML Policy are or become invalid, this shall not affect the validity of the remaining provisions. The Board of Directors may replace the invalid provisions by provisions which are valid and the effect of which, given the contents and purpose of this Code is, to the greatest extent possible, similar to that of the invalid provisions.

* * * * *

ANNEX 1

1. LIST OF DEFINITIONS

1. In this AML Policy, the following terms have the following meanings:

AML means anti-money laundering.

AML Policy means the Anti-Money Laundering Policy of Xcoins.

CDD means Counterparty Due Diligence as described in Clause 7.

Company means (COMPANY), Xcoins, CF Technologies Ltd.

Employee means any director, officer, full-time, part-time and seconded employee including any third-party contractor, who receives or is entitled to receive remuneration for goods or services from Xcoins.

Enhanced Counterparty Due Diligence means the Enhanced Counterparty Due Diligence process as described in Clause 7.7 and further.

General Counsel means the general counsel of JAB.

Governance Framework means the governance framework document of XCOINS as adopted by the Board of Directors.

Xcoins means COMPANY, CF Technologies Ltd.

Board of Directors means the Board of Directors of Xcoins.

MLRO means Money Laundering Reporting Officer

ML means Money Laundering.

Money Laundering means Money Laundering as defined in this AML Policy in Clause 4.

Personnel means the directors, officers, full-time, part-time and seconded employees of Xcoins, and anyone working on XCOINS behalf, e.g. consultants and representatives.

Simplified CDD means the Simplified Counterparty Due Diligence process as described in Clause 7.8.

Standard CDD means Standard Counterparty Due Diligence process as described in Clause 7.6 and further.

Terrorist Financing means Terrorist Financing as defined in this AML Policy in Clause 4.

TF means Terrorist Financing.

2. Save where the context dictates otherwise, in this AML Policy:

   (a) Save where the context dictates otherwise, in this AML Policy unless a different intention clearly appears, a reference to a Clause or Annex is a reference to a clause or annex of this AML Policy;

   (b) words and expressions expressed in the singular form also include the plural form, and vice versa;

   (c) words and expressions expressed in the masculine form also include the feminine form; and

   (d) a reference to a statutory provision counts as a reference to this statutory provision including all amendments, additions and replacing legislation that may apply from time to time.

3. Headings of clauses and other headings in this AML Policy are inserted for ease of reference and do not form part of this AML Policy for the purpose of interpretation.

ANNEX 2

2. FACTORS OF HIGHER RISK SITUATIONS

Factors of higher risk situations

Counterparty risk factors

a. the business relationship is conducted in unusual circumstances;
b. counterparties that are resident in geographical areas of higher risk;

Product, service, transaction or delivery channel risk factors

a. products or transactions that might favor anonymity;
b. non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;
c. payment received from unknown or unassociated third parties; and
d. new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products;

Geographical risk factors

a. countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective anti-money laundering and counter terrorist financing systems;
b. countries identified by credible sources as having significant levels of corruption or other criminal activity;
c. countries subject to sanctions, embargos or similar measures issued by, for example, the
European Union or the United Nations; and
d. countries providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

ANNEX 3

3. FACTORS OF LOWER RISK SITUATIONS

Factors of lower risk situations

Counterparty risk factors

a. counterparties that are resident in geographical areas of lower risk.

Product, service, transaction or delivery channel risk factors

a. products, service, transactions or delivery channel where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (particularly, certain types of electronic money).

Geographical risk factors

a. the counterparty is in one of the Member States of the European Union;
b. the counterparty is in a third country having effective anti-money laundering and counter terrorist financing systems;
c. the counterparty is located in third countries identified by credible sources as having a low level of corruption or other criminal activity; and
d. the counterparty is located in third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent.