**CCX EXCHANGE ANTI MONEY LAUNDERING AND COUNTER TERRORIST FINANCING POLICY**

1. INTRODUCTION

Money laundering and the financing of terrorism have been identified as risks by CCX Exchange (Estonia) 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. Estonia (‘Est’), 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 the cornerstone of AML/CFT obligations for licence holders and outlines the offences and penalties for failing to comply.

The purpose of this AML Policy is designed to articulate our commitment to detecting, preventing and reporting attempts to use the Exchange to illegally launder money, to finance illegal activities such as terrorism and drug trafficking, or to commit fraud (all activities being "Prohibited Activities").

Any questions relating to this policy should be directed to MLRO@ccx.io.

2. Policy Statement

The Company and its board of directors is 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 gambling services.

3. Legal & Regulatory Framework

The principal requirements, obligations and penalties, on which the Company’s Systems and Controls are based, are contained in:

* The Fourth Anti Money Laundering Directive;
* Estonia Proceeds of Crime Act 2017;
* Estonia Counter Terrorism Act 2010;
* Estonia Terrorism Act 2005; and
* Estonia Crimes Act 2011;

4. Money Laundering Offences & Penalties

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.

1. *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.

1. *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 Estonia.

The maximum penalty for this offence on conviction on indictment is fourteen years in prison or a fine or both.

1. *Tipping-off*

A person is guilty of an offence if–

1. he discloses that a money laundering suspicion report has been made or is being contemplated or is being carried out; and
2. 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.

1. *Failure to disclose: relevant financial business*

A person is guilty of an offence if–

1. he knows, suspects or has reasonable grounds to suspect that another person is engaged in money laundering, or is attempting to launder money;
2. 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
3. he does not disclose the information or other matter to the Estonia 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. In addition to the criminal offences and consequences described above, there are also regulatory consequences the Company can face. Potential regulatory action which the Company could face includes:

* Warning;
* Licence suspension and/or revocation;
* Personal management licence review and/or suspension/revocation; and
* Financial penalties i.e.: fines.

5. Terrorism Financing Offences & Penalties

A person commits an offence if he-

1. Raises funds for terrorism
2. Uses and possess money or other property for terrorism
3. Arranges funds for terrorism
4. Arranges the retention or control of terrorism property

The penalty for these offence is fourteen years in prison or a fine or both.

6. Money Laundering Reporting Officer (MLRO)

It is a requirement for all licence holders to appoint an MLRO. The holder of this position, in the Company, is a member of the Compliance & Regulatory Team.

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 mis-use 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 regulatory bodies, 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.

7. 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. 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 ML/TF. 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 Estonia 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.

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.

8. AML/CFT Risk Assessment – Customer Identification (KYC) and Customer Due Diligence

The Company will 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. 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.

Customer Due Diligence (“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 Basic Customer Due Diligence and Enhanced Customer Due Diligence as further explained below.

Know Your Customer (“KYC”) is the process used by the Company to verify the identity of our customers.

As part of our AML Policy, all customers must agree to use the Company’s services that they are prepared to provide any documentation which we find relevant in order to serve our KYC and AML policies, including (but not limited to):

i. Copy of valid official proof of identity of any individual associated with the activity;

ii. Copy of proof of residence not older than 2 months old of any individual associated with the activity;

iii. Reference regarding the source of wealth and/or funds of any individual associated with the activity;

iv. Certificate of incorporation of any legal person associated with the activity;

v. Memorandum & Articles of Association of any company associated with the activity;

vi. List of Shareholders (including ownership structure) and Directors and Signatories of any legal entity associated with your activity;

vii. Certificate of Good Standing stating the registered address, share capital, shareholder(s) and the person/s authorized to represent the legal entity, notarised and apostilled.

viii. Any additional information we may find valid for assessing the risk of offering our services to a particular customer.

If you acting on behalf of a legal entity, the individual will be required to send us the aforementioned KYC documents with a company stamp and certified as a true copy of the original by a lawyer, certifying officer or a Notary public.

The Company also requires that KYC documents to be sent in high quality colour format and reserves the right to reject any documents, which do not comply with the above. In addition, the Company reserves the right to require additional information at any time to verify identification or manage risk.

The Company may also disclose any and/or all of the KYC documents to any relevant authority and/or institution in order to examine, inter alia, the customer’s status concerning bankruptcy, reputation checks and criminal records and/or in order to comply with AML laws, regulations, rules or anything related thereto.

The company also restricts access from certain jurisdictions, type of businesses and certain individuals from becoming our clients and/or consume our services. The AML Policy does not a substitute the customer’s need to comply, in full, with the applicable laws and regulations in connection with their business conduct, personal characteristics and legal status.

The company will review and may change this policy, at their discretion, from time to time in compliance with the applicable laws and regulation framework without notice to customers.

9. 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.

10. Sanctions 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.

11. 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 law enforcement request and/or investigation as well as with the GFSC, the GFIU, the Estonia Royal Police and any other relevant government authority.