iCryptoWorld's AML/KYC POLICIES AND PROCEDURES

This Policy relates to iCryptoWorld's anti-money laundering and countering the financing of terrorism ("AML/KYC") policies and procedures. This Policy is solely for the purpose of providing general information and is not, in any way, legally binding either on www.icrypto.world and/or on any other person(s) (individuals or otherwise).

A. Principles and Approach to AML/KYC Efforts

iCryptoWorld is committed to supporting AML/KYC efforts, in principle, we are committed to, amongst other things:

Individuals appointed to act on our customers ' behalf are exercising due diligence when dealing with our customers.

- Conducting our business in conformity with high ethical standards, and to, as far as possible, guard against establishing any business relations that are or may relate to or may facilitate money laundering or terrorism financing.
- We will, to the fullest extent possible, assist and cooperate with relevant law authorities to prevent the threat of money laundering and terrorism financing.

B. Data processing. Collection of personal information.

1. iCryptoWorld may collect and use the following Personal Information from you to provide services:

- **Full legal name;**
- **Home address, including country of residence;**
- **Email address;**
- **Mobile phone number;**
- **Date of birth;**
- **Proof of identity (e.g., driver's license, passport, or government-issued identity card);**
- **Social Security Number or any comparable identification number issued by a government;**
- **Other** Personal Information that is deemed helpful in verifying whether you are eligible to register on the iCryptoWorld website (provided at the discretion of the client);
- **Other** Personal Information is helpful in ensuring our compliance with legal obligations under applicable anti-money laundering (AML) obligations (provided at the discretion of the client);
- **Other** Personal Information that is required by any court order, any applicable law, administrative regulation, or any order of any other competent government agency (provided at the discretion of the client).

2. iCryptoWorld may also collect, receive, and use the following Personal Information from you to monitor and improve the function of iCryptoWorld website, enhancing your experience in using iCryptoWorld services:

You agree that we collect your information when your login iCryptoWorld website, register on iCryptoWorld website and/or use

the services we provide; you agree to any future revisions to our Privacy Policy by us.

Location Information – Information that is automatically collected via analytics systems providers to determine your location, including your IP address and domain name and any external page that referred you to us, your login information, browser type, and version, time zone setting, browser plug-in types and versions, operating system, and platform;

Log Information – Information generated by your use of iCryptoWorld services that is automatically collected and stored in our server logs. This may include, but is not limited to, device-specific information, location information, system activity, and any internal and external information related to pages that you visit, including the full Uniform Resource Locators (URL) clickstream to, through, and from our Website or App (including date and time; page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page;

User Account Information – Information that is generated by your iCryptoWorld account activities including, but not limited to, instructions regarding funding and disbursement, orders, trades, account balances, and other transactional information;

Correspondence – Information that you provide to us in written or oral correspondence, including opening iCryptoWorld User Account, engaging customer support, and initiating other kinds of communications to contact us; We may receive other information from other third parties, including but not limited to banks or financial institutions that you use for transaction purposes.

3. If you are providing Personal Information of any individual other than yourself to us during your use of iCryptoWorld website and iCryptoWorld services, you promise that you have obtained consent from such individual to disclose his/her Personal Information to us, as well his/her consent to our collection, use and disclosure of such Personal Information under this Privacy Policy.

4. iCryptoWorld will not use your personal information for other purposes, sell or disclose information to any third party (except third-party security partners related to service) without your permission; iCryptoWorld will decentralize your personal information to ensure your data is safely stored in case of the risk of loss, damage, tampering or leakage, etc.

In accordance with local laws and legal procedures, if we are required to provide your personal information by the local government or judicial authority in special conditions, we will disclose your personal information as required.

C. Approach to Risk Assessment and Risk Mitigation

Risk Assessment

We envisage that most of our customers would be retail customers and

that we would as of the date of this Policy, be mainly operating in Hong Kong.

In this regard, we would:

A) document and/or collect documentation in relation to:

1) The identities of our customers.
2) The countries or jurisdictions that our customers are from or in;

B) ensure that to the best of our knowledge, skill, and ability, our customers, connected persons of a customer, natural persons appointed to act on behalf of a customer, and beneficial owners of a customer will be assessed and screened with the assistance of List of Designated Individuals and Entities which include categories such as:

• the Democratic People's Republic of Korea; 2. the Democratic Republic of the Congo; 3. Iran; 4. Libya; 5. Somalia; 6. South Sudan; 7. Sudan; 8. Yemen; 9. The UN 1267/1989 Al-Qaida List; 10. The UN 1988 Taliban List; 11. Persons identified in the First Schedule of the Terrorism (Suppression of Financing) Act (Cap. 325).

Risk Mitigation

If identified, we shall not deal with any persons identified in the List of Designated Individuals and Entities.

D. Our Approach to New Products, Practices, and Technologies

We shall be properly advised, in relation to, identifying and assessing the money laundering and terrorism financing risks that may arise in relation to:

• the development of new products and new business practices, including new delivery mechanisms.
• the use of new or developing technologies for both new and pre-existing

We shall especially pay special attention to any new products and ne w business practices, including new delivery mechanisms, and new or developing technologies, that favor anonymity such as digital tokens (whether security, payment, and/or utility tokens) that favor anonymity.

E. Our Approach to Customer Due Diligence ("CDD")

We do not open, maintain, or accept anonymous accounts or accounts with fictitious names.

We do not establish business relations with or undertake a transaction for a customer that we have any reasonable grounds to suspect that the assets or funds of a customer are proceeds of drug dealing or criminal conduct. We shall lodge a Suspicious Transaction Report and extend a copy to the relevant Financial Intelligence Unit for such transactions.

We perform Customer Due Diligence:

- when we establish business relations with any customer.
- when we have a suspicion of money laundering or terrorism financing.
- when we have doubts about the veracity or adequacy of any information

Identifying our customers

We shall identify each of our customers.
To identify our customers, we shall obtain, at least:

- their full names, including aliases.
- their unique identification numbers (such as an identity card number, birth certificate number, or passport number, or where the customer is not a natural person, their business registration numbers); or
- their registration address, or if applicable, their registered business address, and if different, their principal place of business; and

1) their date of birth, establishment, incorporation, or registration;
2) their nationality, place of incorporation, or registration.

Where a customer is a legal person or legal arrangement, we shall apart from obtaining the relevant information as aforesaid above, identify its legal form, constitution, and powers that regulate and bind the legal person or legal arrangement; we shall also identify connected parties of it (e.g., directors, partners of and/or persons having the executive authority of it), by obtaining at least the following information of each connected party:

- full name, including aliases.
- unique identification number such as identity card number, birth certificate number, or passport number of the connected party).

Verifying the Identities of our Customers

We shall verify our customers' identities using reliable, independent source data, documents, or information. Where our customer is a legal person or legal arrangement, we shall verify the legal form, proof of existence, constitution, and powers that regulate and bind the customer, using reliable, independent source data, documents, or information.

Ongoing Monitoring

We shall monitor business relations with our customers on an ongoing basis. We shall, during business relations with a customer, observe the conduct of the customer’s account and scrutinize transactions undertaken throughout the course of business relations, to ensure that the transactions are consistent with our knowledge of the customer, its business, and risk profile, and where appropriate, the source of funds.

Timing for Verification

We shall complete verification of the identity of a customer before:

- the payment service provider establishes business relations with the customer.
- the payment service provider undertakes any transaction for the customer, where the customer has not otherwise established business relations with the payment service provider.

Where Measures are Not Completed

Where we are unable to complete the measures as required, we shall not commence or continue business relations with any customer or undertake any transaction for any customer.

Where we are unable to complete the measures, the payment service provider shall consider if the circumstances are suspicious to warrant the filing of an STR.

Screening

We shall screen a customer, individuals appointed to act on behalf of the customer, connected parties of the customer, and beneficial owners of the customer against relevant money laundering and terrorism financing information sources, as well as lists and information provided by the Authority for the purposes of determining if there are any money laundering or terrorism financing risks in relation to the customer.

Crystal and Chainalysis

We also use Crystal and Chainalysis systems to perform transaction validations.

F. Our Approach to Enhanced Customer Due Diligence

Politically Exposed Persons

We shall use all reasonable means to determine if a customer, any individuals appointed to act on behalf of a customer, any connected party of the customer, or any beneficial owner of the customer is a politically exposed person, or a family member or close associate of a politically exposed person.

Higher Risk Categories

We recognize that the following circumstances where a customer presents or may present a higher risk for money laundering or terrorism financing include but are not limited to the following:

- where a customer or any beneficial owner of the customer is from or in a country or jurisdiction in relation to which the FATF has called for countermeasures, the payment service provider shall treat any business relations with or transactions for any such customer as presenting a higher risk for money laundering or

terrorism financing; and

- where a customer or any beneficial owner of the customer is from or in a country or jurisdiction known to have inadequate AML/CFT measures, as determined by the payment service provider for itself or notified to payment service providers generally by the Authority or other foreign regulatory authorities, the payment service provider shall assess whether any such customer presents a higher risk for money laundering or terrorism.

We will perform enhanced CDD for a customer who presents a higher risk for money laundering or terrorism financing or any customer the Authority notify us of presenting a higher risk for money laundering or terrorism financing.

G. Our Approach to Bearer Negotiable Instrument and Restriction of Cash Payout

We will not make any payment for any sum of money in the form of a bearer negotiable instrument.

We will not pay any cash in any amount while carrying on our business.

H. Record Keeping

We will keep proper records as required for a time of at least 5 years.

I. Personal Data

We will safeguard the personal data of our customers in the manner prescribed.

J. Suspicious Transactions Reporting ("STR")

We will inform the relevant authorities and file STR Reports as required by law. We will also keep all records and transactions relating to all such transactions and STR Reports.

K. Our Policies on Compliance, Audit, and Training

Amongst other things, we shall appoint an AML/CFT Compliance Officer at the Management Level, maintain an independent audit function, and take proactive measures in regularly training our employees and employees on AML/CFT matters.

L. Enterprise-wide money-laundering/terrorism financing risk assessment

We will employ an enterprise-wide money-laundering/terrorism financing risk assessment in 3 phases:

<u>Phase 1: Assessing inherent risk</u>

We will assess the inherent risk in relation to our:

- customer or entity: we will make an assessment about our

customers and/or entities we deal with.

- geographical level: we will not deal with customers from the List of Designated Individuals and Entities.

Phase 2: Assessing mitigating control

We will assess our mitigating controls about the aforesaid, any and/or all customer(s) whom we find suspicious will be first monitored, followed by exercising enhanced due diligence.

Phase 3: Assessing residual risk

We will assess our residual risks after assessing our mitigating controls.