Cryptex24 KYC/AML/CFT Policy

Version: 1.0.2
Last revised: 19.08.2020

INTRODUCTION

C24 WORLD LTD is a company established under the laws of Seychelles (the "**Company**", "**Cryptex24**", **"we", "our"**). This AML/KYC/CTF Policy (the "**AML Policy**") sets forth the rules and procedures that the Company follows for detecting and preventing any financial crime. These rules apply to all individuals (a physical person or a legal entity incorporated in an appropriate legal form) that enter into contractual relationships with Cryptex24 with regard to the https://www.cryptex24.io website (the "**User**").

The Company is strongly committed to preventing the use of its operations for money laundering or any activity which facilitates money laundering, or the funding of terrorist or criminal activities.

The Company follows two internal procedures (the "**Procedures**"):

1) AML/CTF Procedure for a service of exchanging a virtual currency against a fiat currency;
2) AML/CTF Procedure for a virtual currency wallet service.

The Procedures are administered by the Chief Compliance Officer and his team, together referred to as the **Compliance Department**. The Compliance Department is tasked with monitoring compliance with the relevant AML/CTF Procedures.

According to our AML Policy, Cryptex24 **does not work with** Iran, Sudan, Syria, Democratic People's Republic of Korea, the USA, USA territories: United States Minor Outlying Islands, Puerto Rico, American Samoa, Guam, Northern Mariana Island, and the US Virgin Islands (St. Croix, St. John and St. Thomas).

FRAMEWORK

The Company follows the provisions of the Seychelles Anti-Money Laundering and Countering the Financing of Terrorism Act, 2020 when administrating the Procedures.

PROTECTION MEASURES

Cryptex24 has implemented protection measures, which protect Cryptex24 from involvement in any suspicious financial activity, by:

1) Performing KYC procedures on Users – individuals and legal entities;
2) Performing an enterprise-wide risk assessment to determine the risk profile of the Users;
3) Implementing internal procedures, policies, and controls aimed at mitigating risks of money laundering and terrorist financing;
4) Conducting AML/CTF staff training;
5) Conducting a periodic AML audit;
6) Maintaining and updating User information;
7) Reporting suspicious transactions to the relevant financial authority.

KYC MEASURES

As part of the User Due Diligence, the Company shall:

1) Identify the User or its representative and verify submitted information using reliable, independent sources, including usage of means of e-identification and of trust services for e-transactions;
2) Confirm the authenticity of documents and information provided by Users;
3) Investigate Users, whose activities have been identified as suspicious or risky;
4) Request additional and/or updated documents and information from Users when deemed necessary by the Company;
5) Identify Users on an on-going basis even if Users have been identified in the past.

RISK FACTORS & RISK ASSESSMENT

For the purposes of carrying out the User Due Diligence, the Company reserves the right to request documents and information, which include, but are not limited to:

1) Given name (for natural persons), commercial name & names of directors or other representatives (for legal persons);
2) Date of birth (for natural persons), date of incorporation & company number (for legal persons);
3) Phone number of the User (or its representative in case of legal persons);
4) Country of residence/citizenship (for natural persons) / registered address (for legal persons);
5) Address of residence & document which proves the address of residence;
6) E-mail address;
7) Government-issued ID;
8) Source of funds;
9) Any other document/information, requested by the Company.

USER DUE DILIGENCE LEVELS

Verification levels perform the following functions:

1) Giving access to certain types of deposits and withdrawals;
2) Increasing deposit/withdrawal limits.

The level of verification conducted on the User will influence the number of activities the User can perform on the Cryptex24.

More information on verification levels can be found in KYC/AML Requirements document, which constitutes an integral part of the Cryptex24 AML Policy and is available on the website.

REQUESTED INFORMATION

The list of information and documents are specified in KYC/AML Requirements document, which constitutes an integral part of the Cryptex24 AML Policy and is available on the website.

Certain information will be automatically collected from the documents supplied by the User. The Company reserves the right to request any additional documents and/or information at any time.

HIGH-RISK COUNTRIES WE DO NO WORK WITH

List of "High-Risk" countries: Albania, The Bahamas, Barbados, Botswana, Cambodia, Ghana, Jamaica, Mauritius, Myanmar, Nicaragua, Pakistan, Panama, Uganda, Yemen, Zimbabwe.

List of countries the Company does not work with: Iran, Sudan, Syria, Democratic People's Republic of Korea, the USA, USA territories: United States Minor Outlying Islands, Puerto Rico, American Samoa, Guam, Northern Mariana Island, and the US Virgin Islands (St. Croix, St. John and St. Thomas).

RISK LEVELS

The risk level, as well as the risk factors, are determined according to the Anti-Money Laundering and Countering the Financing of Terrorism Act and the Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism Procedures for Reporting Entities in Seychelles:

Risk Level	Risk Factors
Normal	This level of risk is applicable if no medium-risk and high-risk characteristics are detected
Medium	**This level of risk is applicable if:** 1) The natural person whose residence takes place in the country from the list of "High-Risk" countries and who is performing activities in the countries which are not marked as "High-Risk"; 2) The legal person is situated in the country from the list of "High-Risk" countries or is registered in a low tax rate country, and is performing activities in the countries which are not marked as "High-Risk"; 3) The natural person or the representative of the beneficial owner or shareholder of a legal person is a local Politically Exposed Person or an individual, associated with Politically Exposed Person (i.e. a family member); 4) The legal person's activity area is associated with excessive risk of money-laundering; 5) The legal person's activities are not sufficiently regulated by law, its liability is not clear or legality of its financing is unclear (i.e. trust, civil law partnership, non-profit organization or other contractual legal arrangement).
High	**This level of risk is applicable if:** 1) The User is suspected to be or to have been connected with a financial offense or different suspicious activities; 2) The non-resident User, who is performing activities in the country from the list of "High-Risk" countries; 3) The legal person is suspected to be or ever have been linked with illegal financial or money laundering activities; 4) The legal person is registered outside the European Economic area, whose activity is associated with high risk of money laundering.

RISK FACTORS

Risk Factor	Risk Characteristic
Geographical	1) Country of residence or nationality of the customer is a High-risk country listed in "High Risk" list; 2) The customer is a resident or a citizen of the low-tax or tax-free country.
User	1) The User provides untruthful facts, including but not limited to: discrepancies in provided ID documents, fictitious person,

	stolen identity, counterfeited ID document, post box home address, pervious financial crime record, terrorist record, wanted person etc. 2) The User performs suspicious, high-volume, and unusual transactions.

REASONS FOR DENIAL OF SERVICE BASED ON VERIFICATION PROCEDURE

1) The User is a citizen, resident, and/or incorporated in Iran, Sudan, Syria, Democratic People's Republic of Korea, the USA, USA territories: United States Minor Outlying Islands, Puerto Rico, American Samoa, Guam, Northern Mariana Island, and the US Virgin Islands (St. Croix, St. John and St. Thomas);

2) The user is on any trade or economic sanctions list, including but not limited to the UN Security Council Sanctions list, designated as a "Specially Designated National" by OFAC (Office of Foreign Assets Control of the U.S. Treasury Department) or placed on the U.S. Commerce Department's "Denied Persons List". Cryptex24 maintains the right to select its markets and jurisdictions to operate and may restrict or deny the Services in certain countries at its discretion;

3) The User is a **politically exposed person (PEP)** or a family member of a PEP, which includes natural persons who are or who have been entrusted with prominent public functions, including a head of State, head of government, minister and deputy or assistant minister; members of parliament or of a similar legislative body, members of a governing body of a political party, members of a supreme court, members of a court of auditors or of the board of a central bank; ambassadors, a chargé d'affaires and high-ranking officers in the armed forces; members of an administrative, management or supervisory body of a State-owned enterprise; directors, deputy directors and members of the board or equivalent function of an international organisation, except middle-ranking or more junior officials;

4) The User is younger than 18 years old;

5) Company reserves its right for denial of service based on other factors duly recognized by applicable laws and/or our internal risk management procedures.

MONITORING REQUIREMENTS. SUSPICIOUS ACTIVITY DETECTION AND REPORTING
MONITORING REQUIREMENTS

The Company carries out ongoing monitoring of activities to prevent money laundering, terrorism financing, and other illegal activities.

As part of the monitoring requirements, the Company shall:

1) Check transactions on the Platform;

2) When needed, request documents to update/confirm information gathered when applying client verification measures;

3) When needed, identify the User`s source of funds;

4) Pay additional attention to suspicious, high-volume, and unusual transactions;

5) Pay additional attention to transactions made by Users from high-risk countries.

SUSPICIOUS ACTIVITY DETECTION

In an event that the Company suspects suspicious transactions, as identified in its internal policies and procedures, it shall conduct additional questioning regarding the User activity and request any additional documents that may be required.

SUSPICIOUS ACTIVITY REPORTING

In case the User has not provided information and explanation about the suspicious transaction, a complete set of requested documents, or has presented suspicious or unusual documents that the Company cannot verify, and the Company reasonably suspects that User's activities may be connected to money laundering, terrorism financing, or other illegal activities, the Company shall file a report to the FIU reporting the suspicious activity and reserves the right to suspend the User's account, suspected of such activities at its sole discretion.

All questions regarding the AML/KYC/CTF Procedures conducted on the Cryptex24 Users, can be addressed at: support@Cryptex24.io.