EMCD

KYC/AML External Policy

INTRODUCTION

This External Policy (**KYC/AML Policy**) of EMCD Fintech corp., a private legal entity registered under the laws and regulations of the Panama (**us**, **Company**) is established to prevent and mitigate possible risks of the Company being involved in illegal or illicit activities and to enable Company to meet its legal and regulatory obligations in this area (if any, where applicable).

All terms and definitions used in this KYC/AML Policy that were not defined here specifically must be interpreted in the meaning specified in the general Terms of Service regulating use of the Platform (**General Terms**), and(or) other documents provided on the Platform. If the documents mentioned above also do not define this term, the interpretation of this term is made following the applicable law or the generally accepted meaning.

Any reference to "**you**", "**your**", etc., is interpreted as a reference to the User of the Services.

DEFINITIONS

"***Account***" means the User's personal webpage on the Platform, which the User can only access with the corresponding login-password pair.

"***Company***" or "***we***" means EMCD Fintech corp., a private legal entity registered under the laws and regulations of Panama, reg. 155769566 at PANAMA CITY TOWNSHIP, PANAMA DISTRICT, PROVINCE PANAMA.

"***Digital Assets***" means encrypted or digital assets that, among other purposes, can be used as cryptocurrencies based on blockchain and cryptography technologies and issued and managed in a decentralized form.

"***Partners***" means the legal entities that provide the Services through the Platform and are directly mentioned as providers under the General Terms.

"***Platform***" means a set of information, web forms, software, hardware, and intellectual property objects (including computer software, database, graphic interface design, content, etc.) that can be accessed from various User devices connected to the Internet through special web browsing software (browser) at "https://emcd.io" domain, including domains of the following levels, to get access to the Services.

"***User***" or "***you***" means a registered User of the Platform that confirms all eligibility criteria mentioned herein and accepted provisions of these Terms in addition to the General Terms.

"***KYC/AML verification***" means a verification procedure, the primary purpose of which may be to confirm the identity of the User and the source of the Digital Assets to identify any potential risk of money laundering, terrorism financing, fraud, or other financial crime and comply with AML/KYC legislation requirements. This procedure includes providing additional information and documents by Users to the Company through the Platform and verifying such information and documents by the Company.

1. Purposes and Basis

1.1. The Company is committed to providing its Users a lawful and secure environment. We believe that money laundering and terrorist financing are harmful to the Digital Assets ecosystem and to the legitimate interests of Users. We also know these activities can pose legal and operational risks to Digital Assets activities.

1.2. The Company has a global reach and serves Users in many countries. As a result, we may receive inquiries or requests for information from law enforcement authorities outside of our jurisdiction. We are committed to complying with all applicable laws and regulations, including anti-money laundering and terrorist financing.

1.3. We have robust anti-money laundering and terrorist financing (**AML/CFT**) policies and practices designed to prevent these activities from happening through Services. We take a proactive approach to AML/CFT and are constantly working to improve our systems and procedures.

1.4. The Company comply with requirements set out in the following acts, rules, regulations, and good practice guidelines (Regulating Acts):

- Law No. 23 of April 27, 2015 – Adopting measures to prevent money laundering, terrorist financing, and the proliferation of weapons of mass destruction.
- Executive Decree No. 363 of 2015 – Regulating Law 23 and establishing risk-based approach, record-keeping, and internal compliance program requirements.
- Law No. 70 of 2019 – Strengthening measures to prevent terrorist financing and proliferation of weapons of mass destruction.
- Law No. 11 of 2015 – On international judicial cooperation in criminal matters, including financial investigations.
- Law No. 21 of 2017 – Regulating trust structures under the supervision of the banking regulator.
- Law No. 70 of 2017 – Criminalizing tax crimes as predicate offenses to money laundering.
- Law No. 129 of 2020 – Establishing the beneficial ownership registry.
- Law No. 254 of 2021 – Strengthening accounting record-keeping obligations, regulating the role of resident agents, and enhancing corporate transparency.
- Resolution No. 005/2015 of May 26, 2015 – Complementing Law 23 with due diligence, beneficial ownership identification, PEP controls, cooperation with the Financial Analysis Unit (UAF), KYC policies, and employee protection provisions.
- other documents as may be applicable from time to time.

1.5. Our goal is to be a trusted and reliable partner for our Users. Working together can help create a safe and secure environment for the Digital Assets ecosystem.

2. Scope

2.1. This Policy applies to all Users who use the Services. Users must comply with all applicable AML/CFT laws and regulations in their country or region where they are located. The specific requirements of these laws and regulations will vary from country to country. Users must carefully review the relevant laws and regulations to ensure they follow them.

3. Principles of User Due Diligence

3.1. The Company applies due diligence measures to Users, business relationships, and transactions and monitors business relationships on an ongoing basis.

3.2. Due diligence measures include:

(i) Identifying the User's identity based on documents, data, or information obtained from a reliable and independent source or from any other source that the Company has reasonable grounds to rely on and can be relied upon to identify and verify the User's identity.

(ii) Obtaining information on the purpose and intended nature of the business relationship and establishing details of the User or beneficial owner to enable the Company to identify:

(a) Complicated or unusually large transactions;

(b) Unusual transaction patterns that have no apparent economic or visible legitimate purpose or

(c) Any other activity that, by its nature, may be related to money laundering, terrorist financing, or other criminal conduct.

3.3. The Company applies due diligence when:

(i) It establishes a new business relationship with the User;

(ii) It doubts the accuracy or adequacy of documents, data, or information obtained to identify or verify the User; or

(iii) There is a reasonable suspicion of money laundering, terrorist financing, or other criminal behavior. Notwithstanding the above, the Company applies due diligence measures to existing Users at appropriate times based on User risk.

3.4. The Company applies simplified due diligence measures to specific business relationships or transactions if the Company determines that the business relationship or transaction presents a low risk of money laundering and terrorist financing. Where money laundering and terrorist financing are suspected, the Company does not apply such measures.

3.5. The Company conducts due diligence before establishing and(or) during a business relationship with Users. In some cases, the Company may conduct due diligence on a User after establishing a business relationship, namely where (i) it is necessary in order not to interrupt the normal conduct of business, and (ii) there is no reasonably certain and reasonable suspicion of money laundering or terrorist financing.

3.6. The Company aims to complete the KYC/AML verification process within 3 to 5 business days from the date all required documents are received in full. Additional documents or information may be requested in the following cases:

- If submitted documents are incomplete, unclear, or expired;
- If there is a need to verify the authenticity of documents with issuing authorities;
- If the User's risk profile is classified as medium or high risk;
- If unusual activity or transactions are detected during the review process.

3.7. The User will be promptly notified via the Platform or by email if additional documents or information are required. The User will be informed upon completion of the verification process, including confirmation of successful verification or reasons for rejection. In cases where extended review is necessary, the User will be informed of the updated expected timeline.

3.8. While the Company strives to meet the indicated timelines, certain cases—such as international document verification, high-risk assessments, or requests from regulatory authorities—may require longer processing times.

3.9. The User must provide accurate, complete, and up-to-date information and documents as required for the KYC/AML verification process.

3.10. The User must promptly notify the Company of any changes to the information or documents previously provided, including but not limited to changes in personal identification details, residential address, beneficial ownership, or the nature of business activities.

3.11. The User must cooperate fully with any requests for additional information or documentation during the verification process or during the course of the business relationship, especially in cases where unusual activity is detected or further due diligence is required.

3.12. The User must not attempt to conceal their identity, source of funds, or beneficial ownership through false statements, forged documents, or other misleading actions.

4. Application of Enhanced Due Diligence Measures

4.1. The Company applies risk-based enhanced User due diligence and enhanced ongoing monitoring in addition to due diligence measures in situations that, by their nature, present a higher risk of money laundering, terrorist financing, or other criminal conduct or in relation to business relationships with persons from countries that do not or do not fully apply the Financial Action Task Force (FATF) recommendations.

4.2. The Company considers specific risk factors to decide whether to apply enhanced due diligence measures. Such measures include:

(i) Establishing the source of wealth and the source of funds related to the proposed business relationship or one-off transaction;

(ii) Seeking additional independent, reliable sources to verify the information provided by the Company;

(iii) Taking additional steps to understand the background, ownership, and financial situation of the User and other parties to the transaction.

(iv) Taking further steps to ensure that the transaction is fit for purpose and in line with the intended nature of the business relationship;

(v) Strengthening control over business relationships, including closer monitoring of transactions.

5. Risk Assessment.

5.1. Based on the information gathered via the registration and KYC/AML verification, the Company shall assemble an individual profile of the User upon entry into a business relationship (User Profile). The User Profile shall allow the Company to understand the User's financial background, the origin of the assets involved into transactions, and the purpose of the business relationship, as well as to check their plausibility in terms of legitimacy, or to identify circumstances that require particular clarification. Based on the User Profile the Company shall perform a risk assessment, to determine the User's Risk Profile and the necessary corresponding mitigating due diligence measures to be taken (Risk Profile).

5.2. The risk assessment shall consider the following risk categories, the probability and consequences of their realization and the probability of an increase in the risk:

- geographical risks;
- User-related risks;
- transaction-related risks;
- interface-associated risks.

5.3. Geographical risks, whose factors arise from differences in the legal environment of various countries, these factors may include situation when the User is located in such jurisdiction:

- countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective systems to counter money laundering or terrorist financing;
- countries identified by credible sources as having significant levels of corruption or other criminal activity, such as terrorism, money laundering, and the production and supply of illicit drugs;
- countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;
- countries providing funding or support for terrorism;
- countries that have organisations operating within their territory which have been designated by the Panama, international organisations as terrorist organisations.

5.3.1. The usage of the Company is prohibited for the citizens of the following countries and territories:

- Democratic People's Republic of Korea;
- Islamic Republic of Iran;
- Republic of Iraq;
- Republic of the Sudan;
- Republic of the Union of Myanmar.
- Unrecognized territories, as well as disputed territories: Abkhazia, Donetsk and Luhansk People's Republics, Zaporizhia and Kherson regions, Crimea.

5.3.2. The usage of the Company’s services is prohibited, if a User or a transaction are explicitly connected with the following countries or territories:

- any countries or territories under UN sanctions, and further under any embargo or similar measures;
- countries with insufficient measures for preventing money laundering and terrorism financing.
- countries, which according to reliable sources are involved in terrorism support, or countries with high corruption levels.

5.4. User associated risks, whose factors arise from the person participating in a transaction. These factors may include:

- whether the User is a PEP, family member of a PEP, or known close associate of a PEP;
- the residency of the User, including whether the User is registered in a low tax rate jurisdiction;
- whether the User is included in international sanctions lists;
- circumstances (including those identified in the course of a prior business relationship) resulting from the experience of communicating with the User, representatives and any other such persons;
- whether the origin of the User’s assets or the source and origin of the funds used for a transaction can be easily identified;
- the type and characteristics of the User's business;
- the possibility of classifying the User as a "typical User"; and
- problems during the User’s identification procedures.

5.5. Transaction associated risks, whose factors result from the User's activities or the exposure of a specific product or service to potential ML risks. These factors may include:

- the transaction involves substantial funds or unexplained source of funds;
- the transaction is related to assets or source identified as high risk through the applied transaction screening tool;
- the transaction is part of series of suspicious transactions.

5.6. Interface associated risks, whose factors arise from the channels (mainly the Internet) through which the business relationship is established, and the transactions are carried out, these factors may include:

- whether the channel facilitates anonymity; and
- whether the channel facilitates third party funding.

5.7. The conducted risk assessment shall result in a Risk Profile, identified through the risk factors mentioned in section 5 hereof, and according to the following scale:

5.7.1. Low Risk Profile.

- User is from the Recognized jurisdictions list.

Low Risk Profile includes:

- usage of VPN or TOR browser in case if no other concerns are found;
- different IP with 1.8 proxy.

5.7.2. Medium Risk Profile.

User is:

- not from the countries listed in low risk;
- there are one or more risk factors that differ from the sphere of the "typical" User, but the transaction itself is clear (i.e. there are no risk factors in the transaction associated risks category). At the same time, there is no suspicion that a combination of the risk factors may indicate high risk of ML/TF.
- Depending on the number of risks, the User may be contacted by a company representative (Compliance Department employee) to clarify additional information.

5.7.3. High Risk Profile.

User is:

- from a jurisdiction that, according to credible sources such as mutual evaluations, detailed evaluation reports or published follow-up reports, has not established effective AML/CFT systems;
- from a jurisdiction that, according to credible sources, has significant levels of corruption or other criminal activity;
- from a jurisdiction that is subject to sanctions, embargos or similar measures issued by, for example, the United Nations;
- from a jurisdiction that provides funding or support for terrorist activities, or that has designated terrorist organizations operating within their country, as identified by the United Nations;
- User Profile rises suspicions;
- there are multiple risk factors and the transaction itself is not clear. The combination of these factors cast doubt on the transparency of the User's identity and transactions, indicating of ML/TF.

High risk Profile includes:

- User's birth date 1959 and earlier;
- different Users using the same device/browser.

Proof of residence and source of funds are mandatory for the Users under high-risk category. The Users elderly of age above 65, who are considered high risk Users for scam and may require additional verification from the Company (video verification and/or phone call from one of our representatives).

Where the User's Risk Profile is high in addition to the measures described above, the Company may consider obtaining further verification measures, which shall be approved by the Board/CEO. These may include:

additional documents, data or information originating from a reliable and independent source;
a notarized or officially authenticated copy of the identification documents.

6. Continuous Monitoring

6.1. The Company constantly monitors its Users and their transactions.

6.2. Ongoing monitoring of business relationships means:

(i) Scrutinizing transactions carried out throughout the business relationship to ensure that these transactions are consistent with the Company's knowledge of the User and the risks and source of the User's funds;

(ii) Keeping up-to-date documents, data, or information obtained to apply User due diligence measures.

6.3. All documents, data, and information collected during the KYC/AML verification process will be retained for a minimum of five (5) years from the date the business relationship ends or from the date of the last transaction, whichever is later, in accordance with applicable laws and regulations in Panama and other relevant jurisdictions. In cases where ongoing investigations, regulatory inquiries, or legal proceedings are in progress, the retention period may be extended as required by law.

6.4. All KYC/AML data is treated as strictly confidential and will not be disclosed to third parties except in the circumstances described in this Policy or as otherwise required by applicable law. Employees and contractors with access to User data are bound by confidentiality agreements and subject to disciplinary action in case of non-compliance.

6.5. Data may be shared with:

- Competent regulatory, supervisory, or law enforcement authorities, in response to lawful requests or reporting obligations;
- Financial institutions, payment processors, or service providers engaged in the User's transactions, only to the extent necessary to fulfill contractual or legal obligations;
- Third-party service providers involved in verification processes, provided they meet the Company's data security and confidentiality requirements.

7. Termination Obligations

7.1. Where, in respect of any User, the Company is unable to apply due diligence measures per this Policy, the Company will:

(i) Not carry out the transaction with or on behalf of the User;

(ii) Not establish a business relationship and not carry out one-off transactions with the User;

(iii) Terminate any existing business relationship with the User. If the Company cannot continuously monitor a business relationship, the Company will terminate that business relationship. The Company may sometimes be required to file reports with the relevant authorities.

7.2. Subject to applicable law, Users may request access to their personal data, request correction of inaccurate information, or request deletion of their data after the retention period expires. All such requests will be processed in compliance with applicable data protection regulations.

7.3. The Company reserves the right to refuse to establish a business relationship, to suspend services, or to terminate any existing business relationship with immediate effect if:

- The User provides false, misleading, forged, or altered information or documents;
- The User withholds material information required for the KYC/AML verification process;
- The User attempts to circumvent, manipulate, or otherwise evade the KYC/AML procedures of the Company;
- The User fails to cooperate with the Company in providing requested information or documentation;

- The Company has reasonable grounds to suspect involvement in money laundering, terrorist financing, fraud, or other illegal activities.

Any attempt to bypass, deceive, or obstruct the KYC/AML process will result in the refusal or immediate termination of services, and, where required, will be reported to the competent authorities.

8. International Sanctions

8.1. The Company applies applicable international sanctions and pays special attention to all its Users, their activities, and facts that indicate the possibility that a User is the subject of international sanctions.

9. Policy Amendment

9.1. The Company has the right to amend this AML/CFT Policy. If the current version is amended, the date of the last update of the new Policy will take effect from its publication within the Platform unless otherwise provided for in the new AML/CFT Policy.

10. Contact Us

10.1. If anything is left unclear in the text of this AML/KYC Policy, we will be happy to clarify its provisions. Please get in touch with us via the Platform for any further questions about this KYC/AML Policy or by compliance@emcd.io email.

Last amended on 10.08.2025