

AML/CFT Policy

As we navigate through the modern digital landscape, the cryptocurrency industry faces significant obstacles in the form of money laundering (ML) and terrorist financing (TF). These illicit activities present profound threats to our operations at CRYPTTEOR CAPITAL - FZCO. Acknowledging the magnitude of these threats, we have initiated and executed an all-encompassing Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Policy. Our policy framework is harmonized with the respective laws, industry-standard guidelines, and widely recognized best practices. As a company, CRYPTTEOR CAPITAL - FZCO's commitment to providing reliable, secure, and trustworthy services remains steadfast. We uphold an environment of integrity and transparency while ensuring our full compliance with the applicable laws and international standards.

The essential pillars of our AML/CFT Policy at CRYPTTEOR CAPITAL - FZCO are as follows:

- Know Your Customer/Know Your Business (KYC/KYB) Procedures;
- Customer Due Diligence;
- Risk Assessment and Management;
- Regular and Continuous Monitoring;
- Comprehensive Record Keeping;
- Active and Responsive Communication with Regulatory Bodies.

KYC/KYB Procedures

At CRYPTTEOR CAPITAL - FZCO, we recognize the importance of implementing robust Know Your Customer/Know Your Business (KYC/KYB) procedures to combat identity theft, financial fraud, money laundering, and terrorist financing. This involves a systematic approach to identify our customers and businesses, authenticate their identities, understand their business activities, and effectively assess the potential risks of money laundering associated with each customer.

Customer Due Diligence

A crucial aspect of our operations involves our thorough customer due diligence process. This process allows us to gather essential information about our customers, which is fundamental in assessing and evaluating a multitude of risks. We ensure that this information is procured from the customer prior to the establishment of any business relationships. Furthermore, we validate the obtained information against independent and reliable sources to ensure its accuracy. Our goal is to establish a reasonable belief in the true identity of our customers. This process helps ensure that the customer does not exploit CRYPTTEOR CAPITAL - FZCO's platform for ML or TF. All information, documents, and data supplied during the customer identification process are handled in strict accordance with our stringent Privacy Policy.

Risk Assessment and Management

In our effort to mitigate potential risks, CRYPTTEOR CAPITAL - FZCO employs a risk-based approach. By understanding the range of ML/TF risks to which we may be exposed, we implement our AML/CFT measures in a manner and to an extent that ensures the mitigation of these risks. Our risk-based strategy provides the flexibility to focus our resources and adopt enhanced measures where the risks are higher, thus optimizing our approach to risk management.

Regular and Continuous Monitoring

An integral part of our AML/CFT policy is our commitment to regular and continuous monitoring of all our business relationships with customers. Our rigorous ongoing monitoring is applied uniformly to all customers, irrespective of their risk profile under our risk-based approach. However, the extent and nature of the monitoring are tailored according to the customer's risk rating and the specific service we provide them.

Comprehensive Record Keeping

At CRYPTTEOR CAPITAL - FZCO, we place immense importance on maintaining comprehensive records for every customer. This practice is recognized as a vital component in the fight against ML/TF, primarily because it helps maintain an adequate audit trail, which is an essential aspect of our policy. Effective record-keeping allows for easier investigation, prosecution, and confiscation of criminal assets, thereby hindering the progression of illicit activities.

Active and Responsive Communication with Regulatory Bodies

In instances where there is a suspicion or awareness that any property of value is directly or indirectly a product of criminal activity, or that the property's intended use is to finance terrorists or terrorist organizations, CRYPTTEOR CAPITAL - FZCO takes immediate action. We promptly report such activities to the relevant authorities and cooperate fully in all subsequent actions, reinforcing our commitment to active and responsive communication with competent regulatory bodies.

Screening and Monitoring Process

Cryptteor Capital employs a rigorous Screening and Monitoring Process to ensure compliance with Anti-Money Laundering (AML) regulations. Our process includes:

- **Customer Identification and Verification:** We collect sufficient information to establish the identity of our customers. This includes verifying customer's identity using reliable, independent source documents, data, or information.

- **Watchlist Screening:** All customers are screened against global watchlists, including OFAC (Office of Foreign Assets Control), UN, EU, and other relevant sanctions lists as well as databases for PEPs.
- **Transaction Monitoring:** We conduct continuous surveillance of customer transactions to identify patterns that may indicate money laundering or terrorist financing activities. Any suspicious transactions are escalated for review and, if necessary, reported to the relevant authorities.
- **Enhanced Due Diligence:** For high-risk categories, enhanced due diligence measures are applied, including obtaining additional information on the customer and their business relationships.

In-depth Risk Assessment

Our in-depth Risk Assessment framework involves:

- **Risk Scoring:** Assigning risk scores based on a variety of factors, such as the nature of the business, source of funds, customer's geographic location, and transaction behavior.
- **Regular Reviews:** Conducting periodic reviews of the risk assessment to capture any changes in the customer's risk profile or operational practices that may affect their risk rating.
- **Customized Controls:** Implementing control measures tailored to the risk level of specific customer groups, accounts, and transaction types.

Geographical Risks

Crypteor Capital acknowledges that certain geographical regions pose higher risks due to the prevalence of corruption, conflict, or weak AML/CFT measures. We undertake additional measures, including:

- **Country Risk Classification:** Assigning risk levels to countries based on reliable and up-to-date information from international bodies and local sources.
- **Enhanced Measures for High-risk Jurisdictions:** Applying enhanced due diligence for any customer residing in or conducting transactions with high-risk countries.

Prohibited Jurisdictions

To maintain the integrity of our operations and comply with international AML/CFT standards, Crypteor Capital does not provide services to individuals or entities located in or conducting transactions with the following prohibited jurisdictions:

- Belarus
- Cuba
- Crimea
- Democratic Republic of Congo

- Iran
- Iraq
- North Korea (DPRK)
- Sudan
- South Sudan
- Syria
- Zimbabwe
- Russia
- Georgia
- Ukraine (excluding the provision of humanitarian aid, legal services, and internet communications)
- Moldova
- Armenia
- Azerbaijan
- Kazakhstan
- Uzbekistan
- Turkmenistan
- Kyrgyzstan
- Tajikistan

These jurisdictions are identified as having strategic deficiencies in their AML/CFT regimes or are subject to sanctions, embargoes, or similar measures. Crypteor Capital reserves the right to update this list in response to changes in international law and the global political climate.

