

Grand Time

KYC/AML/CFT Policy

Version: 1.01
Last revised: 27.07.2021

INTRODUCTION

Grand Time Group LTD is a company established under the laws of Seychelles (the “**Company**”, “**Grand**”, “**we**”, “**our**”). This KYC/AML/CFT Policy (the “**AML Policy**”) sets forth the rules and procedures that the Company follows for detecting and preventing any financial crime during the Website use and/or Grand Token Sale.

These rules apply to all individuals (a physical person or a legal entity incorporated in an appropriate legal form) that enter into contractual relationships (the “**User**”) with the Company with regard to the <https://grandtime.org/> Website use and/or participation in the Grand Token Sale.

This AML Policy is part of the agreement between you and us, Grand Token Sale Terms and Conditions (the “**Terms and Conditions**”). Unless explicitly stated otherwise, the terms in this AML Policy have the same meaning as in the Terms and Conditions.

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.

According to our AML Policy, the Company **does not work with the following countries**: Democratic People’s Republic of Korea, Iran, Cuba, and Syria (the “**Prohibited Countries**”).

THE COMPANY RESERVES ITS RIGHT TO SET FORTH AT ANY TIME UPON ITS OWN DISCRETION SPECIAL ELIGIBILITY OR OTHER REQUIREMENTS TO CERTAIN USERS TO PARTICIPATE IN A CERTAIN PHASE OF THE GRAND TOKEN SALE AS SHALL BE MENTIONED ON THE WEBSITE AND WHITE PAPER.

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

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

- 1) performing KYC procedures on its 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/CFT 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 the Users;
- 3) investigate its 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 said 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 beneficiaries, 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) email address;
- 7) government-issued ID (for natural persons) / constitutional document; (for legal persons)
- 8) source of funds;
- 9) any other document/information, requested by the Company.

REQUESTED INFORMATION

Certain information will be automatically collected from the documents supplied by the User.

The list of information and documents that is requested by the Company:

Tokens Purchased / Information & Documents	Tokens for an equivalent of up to \$3,300.00	Tokens for an equivalent exceeding \$3,300.00
E-mail	✓	✓
Full name / Company name & names of directors, representatives and/or end-beneficiaries	✓	✓
Date of birth / Registration date	✓	✓
Gender / Company number	✓	✓

Country of citizenship / incorporation	✓	✓
Government-issued ID / Constitutional document	✓	✓
Selfie with the ID (for natural persons only)	✓	✓
Home address / registered office address	-	✓
Information as to the source of funds	-	✓ (at the discretion of the Company upon conducting risk assessment)

DOCUMENT REQUIREMENTS:

ID – a government-issued Passport, ID card, Driving License, Residence Permit.

Source of funds – the non-exhaustive list may include contract of sale, income certificate, tax certificate no older than 3 months from the date of issue etc.

The Company reserves the right to request any additional documents and/or information at any time.

HIGH-RISK COUNTRIES WE DO NOT WORK WITH

We **do not work** with the countries from the following lists:

- high-risk jurisdictions according to the latest FATF public statements (<http://www.fatf-gafi.org/countries/#high-risk>);
- countries-sponsors of terrorism (<https://www.state.gov/state-sponsors-of-terrorism/>);

which altogether include countries, such as **Democratic People's Republic of Korea, Iran, Cuba, and Syria**.

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) a 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";

	<p>2) a 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”;</p> <p>3) a 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 a Politically Exposed Person (i.e. a family member);</p> <p>4) a legal person’s activity area is associated with excessive risk of money-laundering;</p> <p>5) a 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).</p>
High	<p>This level of risk is applicable if:</p> <p>1) a User is suspected to be or to have been connected with a financial offense or different suspicious activities;</p> <p>2) a non-resident User, who is performing activities in the country from the list of “High-Risk” countries;</p> <p>3) a legal person is suspected to be or ever have been linked with illegal financial or money laundering activities;</p> <p>4) a legal person is registered outside the European Economic area, whose activity is associated with high risk of money laundering.</p>

RISK FACTORS

Risk Factor	Risk Characteristic
Geographical	<p>1) the country of residence or nationality of the customer is a High-risk country listed in “High Risk” list;</p> <p>2) a User is a resident or a citizen of a low-tax or tax-free country.</p>
User	<p>1) a 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, previous financial crime record, terrorist record, wanted person etc.</p> <p>2) a User performs suspicious, high-volume, and unusual transactions.</p>

REASONS FOR DENIAL OF SERVICE BASED ON VERIFICATION PROCEDURE

- 1) the User is a citizen, resident, and/or incorporated in Democratic People’s Republic of Korea, Iran, Cuba, Syria;
- 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. The Company 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) the 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 Website;
- 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's 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 KYC/AML/CFT Procedures conducted on the Grand Website Users can be addressed at: support@grandtime.org.