Anti Money Laundering and Counter-Terrorist Financing Policy of QWorld Association

Adopted by the General Meeting on 29. 06. 2026.

1. Purpose and Scope

The QWorld Association (hereinafter "the Association") is committed to the highest standards of integrity and transparency. This Policy establishes a framework to prevent the Association and its projects from being used, even inadvertently, for money laundering or the financing of terrorism.

This Policy is binding for:

1. Members of the Management Board.
2. The Financial Controller.
3. The operative boards of each project established by the General Meeting.
4. Any member or volunteer authorized to handle financial transactions, negotiate sponsorships, or manage project-specific budgets.

2. Compliance

This document is aligned with the principles established by the **Estonian Money Laundering and Terrorist Financing Prevention Act** and the guidelines provided by the Estonian Financial Intelligence Unit (FIU). It is adopted to ensure the Association operates according to international best practices, including adherence to global sanction regimes, and maintains the highest levels of institutional and financial integrity.

3. Internal Governance and Responsibility

1. **Ultimate Responsibility:** The Management Board (MB) is legally responsible for the implementation of this Policy and ensuring the Association remains compliant with Estonian AML/CTF regulations.
2. **Operative Management:** The operative management boards of each project is responsible for ensuring that all thematic and departmental activities adhere to these standards.
3. **The Compliance Liaison:** The **Financial Controller** is designated as the internal AML Liaison Officer. Their duties include:

- Monitoring the flow of funds for unusual patterns across all Association activities.
- Ensuring that "Know Your Counterparty" (KYC) documentation is collected for significant transactions.
- Reporting suspicious activities to the Management Board and relevant project leads for further evaluation.

4. "Know Your Counterparty" (KYC) and Due Diligence

The Association shall perform due diligence on all significant financial contributors, sponsors, and grant-making bodies.

1. **Standard Due Diligence:** For any transaction or cumulative annual payments exceeding **€1,000**, the Association must verify the identity of the counterparty (National ID or Passport for individuals; Corporate Registry for entities.
2. **Enhanced Due Diligence (EDD):** For transactions exceeding **€10,000**, or if the counterparty is based in a "High-Risk Third Country" as defined by the European Commission or in a country on the FATF Grey/Black list, the Association must:
    - For organisations Identify the Beneficial Owners.
    - For individuals maintain a copy of government-issued ID and proof of residence.
    - Screen names against international Sanction Lists, specifically including the UN, EU, Estonian national sanctions, and the OFAC lists.

5. Disbursement Controls and Proof of Work (PoW)

To prevent "ghost consulting" or illicit fund transfers, the following controls apply to all outgoing payments:

1. **Standardized Invoicing:** Every payment request must be accompanied by a formal invoice containing the recipient's full name, address, tax ID (if applicable), accompanied by a document describing in detail the work performed.
2. **Bank Account Matching:** Funds must only be sent to a bank account held in the name of the contracted individual or entity. Third-party payments are strictly prohibited.

6. Prohibited Activities

1. **Anonymous Donations:** No anonymous donation exceeding €100 shall be accepted.
2. **Cash Transactions:** The Association operates on a "Digital Only" basis. Acceptance of cash is strictly prohibited.
3. **Sanctioned Entities:** No funds shall be accepted from, or paid to, any individual or entity appearing on relevant EU, UN, or US OFAC sanction lists.

7. Red Flags and Suspicious Activity

Management and project leads must be alert to "Red Flags," including:

* Incoming funds from entities with no verifiable online presence, physical address, or legitimate business purpose.
* Payments received or made for invoices that lack a clearly defined or documented delivery of service, or instances where the invoiced amount is significantly higher or lower than the fair market value of the service.
* Requests to refund a donation to a different account than the source.
* Payments for "expert services" that are significantly above market value.
* Frequent or large-scale payments from entities whose primary business activity is unrelated to the quantum ecosystem or the Association's mission.

8. Reporting Obligations

1. **Internal Reporting:** Any suspicion of money laundering must be reported immediately to the Chairperson of the Management Board.
2. **External Reporting:** Credible suspicions must be filed by the Management Board with the Estonian Financial Intelligence Unit (FIU).
3. **No Tipping Off:** It is a criminal offense to inform a counterparty that a suspicious activity report has been filed against them.

9. Record Keeping

All documentation related to KYC and AML screenings must be kept for at least **five (5) years**.

10. Governance and Review

1. **Authority:** This Policy is the competence of the **General Meeting**. Any creation, substantial amendment, or revocation of this Policy must be approved by the General Meeting.
2. **Annual Review:** The Management Board shall present this Policy for review at the annual General Meeting to ensure continued alignment with evolving Estonian, European Union, and international standards.

Gábris Aurél

Digitally signed by GÁBRIS,AURÉL GÁBOR,37712200490
Date: 2026.07.18 20:08:31 +02'00'