ANTI-TERRORISM AND ANTI-MONEY LAUNDERING POLICY

Approved by Board of Directors 2022-01-18

The Objective

Child10 is determined to prevent its funds from being used directly or indirectly for terrorist activities and to prevent that the proceeds of crime can be washed through Child10. Funds that are diverted to terrorist organizations or used for criminal acts are funds that do not reach the intended projects, programs, and beneficiaries and, therefore, the most vulnerable will suffer. Further to this, suggestions that an NGO is linked to terrorism or money laundering in any way can be damaging to its reputation and undermine the trust and support of beneficiaries, partners, the wider public and donors. The objective of this policy is to prevent Child10 funding terrorism, breaching sanctions, or being used as a vehicle for money laundering.

Scope

The policy applies to the organization as well as to all staff members and consultants of Child10. All partners, donors and suppliers are subject to the measures to prevent financing terrorism and/or money laundering.

Whilst we work mainly in low-risk locations for terrorism, Child10 works with and share resources with local partner organizations, the majority of whom we have done due diligence on as part of our Child10 award process. Some we have known well over a long period of time. We believe that, by working in this way, there is a relatively low risk that our funds will inadvertently find their way into the hands of those who will use them for violent purposes. However, given the impact of any proven or alleged terrorist funding, Child10 takes several measures in its process to select partner organizations, suppliers and donors to further reduce this risk.

Dissemination

The Anti-terrorism and anti-money laundering policy is openly available on Child10 ’s external websites and the organization’s internal document library. All updates will be communicated to all Child10 staff, partners, donors and consultants. Critical checks of the policy are part of the annual policy oversight process, and of the onboarding program of all new staff members. The Anti-terrorism and anti-money laundering policy is mentioned in (and linked to where deemed applicable) legal agreements with partner organizations, donors, consultants and suppliers.

Related policies, process descriptions, procedures and tools

This policy should be read in connection with the following Child10 policies, process descriptions, procedures, and tools:

Policies:

- Code of Conduct
- Fundraising and Partnerships policy
- Procurement policy
- Annual Risk Assessment
- Irregularity & Misconduct policy

Checklist:

- Due Diligence Process checklist

Definition

A terrorist act is an act, or a threat to act, that meets both these criteria:

• Terrorism intends to coerce or influence the public or any government by intimidation to advance a political, religious or ideological cause.

• Terrorism causes one or more of the following: death; serious harm or danger to a person; serious damage to property; a serious risk to the health or safety of the public; and serious interference with, disruption to, or destruction of critical infrastructure such as a telecommunications or electricity network.

Advocating, protesting, dissenting, or taking industrial action are not terrorist acts where the person doing the activity does not intend to cause serious harm to a person or create a serious risk to public safety. Money laundering is the process by which the proceeds of crime are channeled through financial systems to disguise their illegal origin and returned to the launderer in an indirect manner.

Prevention

Child10 has the following measures in place to reduce the risk of accidentally and deliberately funding of terrorism or being used for money laundering:

Due Diligence on partners, suppliers and donors: Child10 has a Fundraising & Partnerships policy and a Code of Conduct that prescribes the limitations to the type of organizations with whom we cooperate. For all new partner organizations a partner risk assessment is performed (following the Due Diligence Process checklist), indicating the different risks of working together with this partner. Based on the assessment, risk mitigating measures are taken to reduce the identified risks. To make sure that Child10 does not enter into financial relations with terrorist or criminal organizations, new partners, suppliers, and donors go through a background check. Donors never decide to which organizations or individuals their funds are paid. In case checks reveal potential risks in relation to terrorism or money laundering, additional research will be done. Only when additional research gives guarantees, can cooperation with the organization be considered.

Code of Conduct: Child10 enforces a Code of Conduct among its staff and its contract partners. Staff and contract partners sign up to the Code of Conduct on joining the organization or when signing a

contract with Child10. The Code of Conduct specifically mentions that staff and contract partners should contribute to preventing unethical and criminal activities.

Procedures: Child10 has signatures and/or system workflow approvals that are required at different stages in any financial transaction process to avoid unauthorized transactions.

"Three lines of defense"-internal control system: Child10 has an internal control system that follows the "three-lines-of-defense"-approach. The first line is the policies, processes, and procedures for the management of operations. The second line is the risk management processes which seek to identify gaps and exposures through an annual risk assessment. The third line is the audit function, which independently monitors these first two lines.

Budget management: Budget versus actual expenditure reports are prepared and reviewed with senior management on a monthly basis. A consolidated report is shared with the Board of Directors several times a year. Budgets are maintained in the accounting system. In addition, Child10 retains all supporting documentation (receipts, invoices and supporting documents) in line with legislative requirements.

Cash and Bank management: Controls include monthly bank reconciliations, checks on authorization levels to carry out financial operations, segregation of duties, signatures and system approvals. In addition, all bank transfers require dual signatures.

Detection

Annual external audit and external project audits: Child10 undergoes an annual external audit of its financial statements and management of the foundations assets and liabilities.

Monitoring & reporting

All incidents of possible criminal activities that are proactively and/or retroactively noticed within Child10, will be reported to the Secretary general and the Chairman of the Board of Directors. Suspicions of financing terrorism and/or money laundering will be dealt with by the Board of Directors and follow the same routing as suspected fraud, including possible sanctions, as per Child10's Irregularity & Misconduct policy.

Responsibilities

The Board of Directors is the owner of this Anti-terrorism and anti-money laundering policy and approves the policy. The Secretary general is responsible for keeping this procedure up to date and review the policy at least on an annual basis. CFO support is consulted when updating the policy.

All staff will be informed through staff meetings or email on updates of the policy.