ANTI-MONEY LAUNDERING POLICY OF

[NAME OF NGO (“[NGO]")

*This policy template and its contents are for general information only. It is not, and is not intended to, constitute legal advice, and should not be relied on as such. The purpose of this template is to assist non-government organizations (NGOs) design and implement their own operational procedures regarding anti-money laundering. NGOs should tailor this template protocol to their own operations and management structure.*

*The information contained in this template is not intended to provide, nor should it be relied on as, any legal advice. While PILnet endeavors to ensure that the information contained in this document is accurate as at the time of publication, neither PILnet nor any of its partners, employees, or agents make any representation or warranty (express or implied) or accept or will accept any responsibility or liability in relation to the accuracy or completeness of the information contained in this document. Any responsibility or liability in respect of any such information or any inaccuracy in this document or omission from this document is expressly disclaimed.*

*Note that this policy template assumes that the Hong Kong-based NGO adapting the policy is not providing products or services which are themselves specifically regulated for AML purposes by a Hong Kong regulator under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615)– e.g. financial services (including banking, securities, etc), insurance, legal services, accounting services, trust and corporate service providers.*

TABLE OF CONTENTS

Page

[1. Policy Statement and Purposes of this Policy 1](#_Toc56450473)

[2. Application of this Policy 1](#_Toc56450474)

[3. Money Laundering and Terrorist Financing in Hong Kong 1](#_Toc56450475)

[4. Risk Assessment of [NGO]’s Activities 4](#_Toc56450476)

[5. Donor Due Diligence 5](#_Toc56450477)

[6. Beneficiary Due Diligence 11](#_Toc56450478)

[7. Partner due diligence 12](#_Toc56450479)

[8. Third party transactions 13](#_Toc56450480)

[9. Compliance Officer/Money Laundering Reporting Officer 13](#_Toc56450481)

[10. Suspicious Transaction Reports 14](#_Toc56450482)

[11. Record Keeping 16](#_Toc56450483)

[12. Staff Training 16](#_Toc56450484)

# Policy Statement and Purposes of this Policy

## [NGO] takes a zero-tolerance approach to money laundering and terrorist financing activities and is committed to implementing and enforcing effective internal controls to counter such activities.

## [NGO]’s policy is to apply at a minimum the standards set out in this Policy.

## The purpose of this Policy is to:

### set out the responsibilities of [NGO] and its [trustees, advisors and] all staff working for [NGO], whether on a paid or voluntary basis (together “**[NGO] Individuals**”), in respect of observing, complying with, and upholding policies on anti-money laundering (“**AML**”) and counter-terrorist financing (“**CTF**”); and

### provide information and guidance to [NGO] Individuals on the money laundering/terrorist financing risks arising in relation to [NGO]’s activities, [NGO]’s due diligence procedures, and how to recognise and deal with any potential money laundering/terrorist financing issues if they arise.

## This Policy may be amended from time to time to reflect updates to the laws and regulations on which it is based.

# Application of this Policy

This Policy applies to all [NGO] Individuals, including those working with [NGO] on a purely voluntary basis. [NGO] will terminate its involvement with any [NGO] Individuals who fail to comply with this Policy.

# Money Laundering and Terrorist Financing in Hong Kong

## Money Laundering (“**ML**”)

### Under Hong Kong law, the term “money laundering” refers to an act intended to have the effect of making any “property” (defined broadly to include any tangible or intangible financial benefit) that represents the proceeds obtained from the commission of a crime appear not to represent such proceeds. Put another way, money laundering is the process of disguising or “cleaning” money directly or indirectly arising from criminal activity (i.e. “dirty money”) so as to conceal its criminal origins.

### The criminal activity in question must either be (a) an “**indictable offence**” under the laws of Hong Kong, or (b) any conduct which, if it had occurred in Hong Kong would constitute an indictable offence under the laws of Hong Kong.

### ML generally consists of three common stages:

#### **placement** - the physical disposal of cash proceeds derived from illegal activities into the financial system, or conversion of funds already in the financial system into the proceeds of crime (e.g. tax evasion, payments made for corrupt or criminal purposes);

#### **layering** - separating illicit proceeds from their source by creating complex layers of financial transactions, often with no legitimate commercial purpose, designed to disguise the source of the money, subvert the audit trail and provide anonymity; and

#### **integration** - returning the laundered proceeds back into the general financial system in a way so that they appear to be the result of, or connected to, legitimate business activities.

### The primary ML offences under Hong Kong criminal law are set out in the **Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405)** and the **Organized and Serious Crimes Ordinance (Cap. 455)** (together, the “**ML Statutes**”). All individuals in Hong Kong are subject to this statutory framework.

#### **“Dealing” with criminal property**: it is an offence for a person who, knowing or having reasonable grounds to believe that any property which, in whole or in part, directly or indirectly represents the proceeds of crime, “deals” with that property. “Dealing” covers a wide range of activity, including receiving or acquiring, concealing or disguising, disposing or converting, or using the property as security (e.g. for a loan).

#### **Failure to disclose**: it is an offence for a person who knows or suspects that any property (in whole or in part, directly or indirectly) represents the proceeds of crime or was otherwise used, or is intended to be used, in connection with an indictable offence, to fail to disclose that knowledge or suspicion to an authorized officer as soon as it is reasonable to do so. In other words, there is a statutory “duty to report” knowledge or suspicion of ML.

#### **Tipping off**: it is an offence for a person who knows or suspects that a report has been made under sub-para (ii) to disclose that fact to any other person (e.g. to the individual suspected of being involved in ML) in a manner which is likely to prejudice any investigation which might be conducted by law enforcement as a result of the original report.

### Although not strictly part of the HK ML statutory framework, the **Hong Kong National Security Law and its Implementing Rules** **(“NSL”)** should also be considered by [NGO].

#### The following acts are criminal offences under the NSL: secession, subversion, terrorist activities, and collusion with a foreign country or external elements to endanger national security (“**Offences”**).

#### The Offences under the NSL would also be considered as “indictable offences” under the ML Statutes (refer to section 3.1(a)-(b) above). This means that an NGO which “deals” with donations which they know or have reasonable grounds to believe are the proceeds of an Offence under the NSL would be committing a separate offence under the ML Statutes.

#### Similar to the provisions under the Hong Kong ML statutes (see section 3.1(d)(ii) above), the NSL includes an obligation that requires an individual to make a report to law enforcement if they “know” or “suspect” that any property is “Offence related property.”

#### “**Offence related property**” as defined in the NSL refers to the property of a person who commits or attempts to commit, or participates in or facilitates the commission of, an Offence; or property used / intended to be used for financing or assisting the commission of an Offence. Note that the definition covers a wide range of property associated with a person arrested/charged under the NSL, regardless of the share owned/controlled by that person.

#### Scenarios which would trigger the disclosure obligation include (but are not limited to) an NGO learning that a person has been arrested for/ charged for an Offence; and/or an NGO having knowledge or suspicion that funds/assets are Offence related property after receiving information from law enforcement agencies. The procedures described in Section 10 (“Suspicious Transaction Reports”) of this Policy will also apply to reports made under the NSL.

## Terrorist Financing (“**TF**”**)**

### TF takes place when funds from either legitimate or criminal sources (or a combination of the two) are used to encourage, plan, organize, or commit a terrorist act, participate or threaten to participate in terrorist activities, or to otherwise benefit a terrorist or terrorist organisation. In TF, the focus is on the end use of the funds in question, whereas with ML, the focus is on the origin of the funds.

### Hong Kong legislation prohibits terrorist financing or otherwise providing material support to terrorists under the following statutes:

#### **United Nations (Anti-Terrorism) Measures Ordinance (Cap 575) (“UNATMO”)**; and

#### The Hong Kong National Security Law.

### Definitions

#### “Terrorist Act” / “Terrorist Activities”

##### Both UNATMO and the NSL capture the same general type of activity under its definitions of “terrorist act” (UNATMO) and “terrorist activities” (NSL) – namely, activities causing or threatening to cause serious violence or harm against a person, property (public or private), or essential public services with the intent to compel the governments of Hong Kong or the PRC or an international organization, and/or intimidate the public, for the purpose of advancing a political, religious or ideological cause.[[1]](#footnote-2)

##### Note that in the case of the NSL, the “terrorist activities” in question cover those causing or intending to cause grave harm to society with the view to coercing the PRC or Hong Kong SAR or the public to “pursue a political agenda” – e.g. encouraging the secession of Hong Kong from the PRC.

#### “Terrorist” / “Terrorist Organization”/ “Terrorist Associate”

##### UNATMO defines “terrorist” as a person who commits or attempts to commit, or who participates in or facilitates the commission of, a terrorist act, and “terrorist associate” as an entity owned or controlled by a terrorist. While the NSL does not define “terrorist”, it does define “terrorist organization” as any organization that commits, intends to commit, or participates or assists in the commission of, “terrorist activities” as defined under the NSL. It is reasonable to draw the inference that persons involved in “terrorist organizations” under the NSL will likely be considered “terrorists” under that law.

### UNATMO prohibits “terrorist financing” which it deems to occur when an individual (i) provides or collects property, with the intention or knowing or having reasonable grounds to believe, that the property will be used to commit one or more terrorist acts, or (ii) makes property or financial services available to, or for the benefit of, a terrorist or terrorist associate. Similarly, the NSL prohibits providing “material support” – including funds and other tangible or intangible support – to terrorist organizations, terrorists, or terrorist activities.

# Risk Assessment of [NGO]’s Activities

## Overview

### While there is not widespread evidence of Hong Kong charities and NGOs being actively compromised by ML and TF activities, the sector remains vulnerable to such activities because of the inherent risks related to fund raising, relatively high cash turnover, and provision of charitable funds/services. This vulnerability is exacerbated by the fact that most charities and NGOs have limited financial resources, which in turn means that they have less to spend on internal administration, governance and compliance processes. Criminals and terrorists are aware of these circumstances and may seek to exploit them.

### Internationally, there have been a number of examples of NGOs and charities being exploited by terrorist organizations to provide financial and logistical support for their operations. These cases have led to a particular focus on the NGO and charitable sector by governments and regulators. According to the Hong Kong government’s 2018 ML and TF risk assessment report[[2]](#footnote-3), there is no indication that the Hong Kong NGO and charitable sector have been involved in any local activities related to TF. To the extent that any local NGOs or charities are involved with charitable activities outside of Hong Kong (e.g. in conflict zones or areas in which terrorist groups are known to operate), they should be aware that there may be elevated TF or ML risk arising from such activities (e.g. from cross-border fund flows).

### It is important for NGOs and charities to be aware of these risks so that they can not only take active steps to mitigate these risks and prevent themselves from being misused by criminals and terrorists, but also so that they understand why financial institutions (for example) may consider the sector as potentially higher risk for ML and TF.

### The Hong Kong government has produced guidance for NGOs and charities on TF: “An Advisory Guideline on Preventing the Misuse of Charities for Terrorist Financing”, published by the Hong Kong Narcotics Division of the Security Bureau (dated September 2018); see link in footnote.[[3]](#footnote-4)

## NGOs and charities can be misused by money launderers or other criminals in a variety of ways, including (but not limited) to the following:

### A donor loans or gives a significant amount of cash to an NGO/charity as a way to dispose of the proceeds of crime;

### A donor makes a donation with a request/condition that the funds be passed by the NGO/charity to a specific individual or group who may appear legitimate but is actually involved in ML or TF activities;

### A recipient or beneficiary of NGO/charitable funds use the funds received for ML or TF purposes;

### A partner organization of the NGO/charity with whom the NGO/charity shares funds and/or resources is involved (without the knowledge of the charity) in ML or TF activities.

## The primary risk for NGOs and charities in this regard is a criminal posing as a genuine donor or beneficiary. Refer to **Appendix A** for a non-exhaustive list of circumstances which would indicate a higher risk of ML/TF relating to a potential donor, beneficiary or partners (“**Higher Risk Factors**”).

## In light of the elevated risks highlighted associated with receiving and providing donations, [NGO] will undertake appropriate due diligence in accordance with the terms of this policy when reviewing donors, beneficiaries, and any partner organizations.

# Donor Due Diligence

## The donor due diligence exercise is the process by which potential donors are screened to assess whether they present a material ML/TF risk. It involves identifying the donor, verifying their identity, and undertaking high-level media screening. The due diligence process also enables [NGO] to check that the donor’s profile is consistent with the purpose and objectives of [NGO]. The process should be **risk-based**, meaning that the higher the risk of ML/TF presented by the donor, the more extensive the due diligence process should be. The risk-based approach ensures that disproportionate time is not spent reviewing low value/low risk donations.

## [NGO] will conduct due diligence as set out in this Section 5 in line with the following guidelines, bearing in mind that the application of a risk-based approach may require flexibility in individual cases: [[4]](#footnote-5)

### Standard due diligence (refer to section 5.5): *[see drafting note in footnote]*

#### Domestic donations with no Higher Risk Factors and/or other reasons for suspicion: donations originating in Hong Kong which will be used to benefit individuals or communities in Hong Kong- donations over HKD [50,000];

#### Donations with an international element with no Higher Risk Factors and/or other reasons for suspicion: donations originating from outside Hong Kong and/or those intended to be used to benefit individuals or communities outside of Hong Kong- donations over HKD [25,000];

#### Donations with a single Higher Risk Factor (other than sanctions or Politically Exposed Person (PEP) risk - see section 5.5(b) and (c)), regardless of whether domestic or international): donations over HKD [25,000][[5]](#footnote-6);

### Enhanced due diligence (refer section 5.6):

#### Donations equal to or in excess of HKD [120,000];

#### Donations with potential sanctions or PEP risk; and/or

#### Donations with multiple Higher Risk Factors or which otherwise are atypical, unusual or suspicious in the experience of [NGO].

### Summary table

|  |  |  |
| --- | --- | --- |
| **Nature of donation** | **Monetary Threshold over which Due Diligence should be completed** | **Type of Due Diligence** |
| Domestic only – e.g. originates from Hong Kong resident and will be used to benefit Hong Kong beneficiaries/society + no Higher Risk Factor (refer to Appendix A for examples) | HKD [50,000] | Standard |
| International – e.g. originates from a donor outside of Hong Kong and/or is intended benefit beneficiaries/communities outside of Hong Kong + no Higher Risk Factor | HKD [25,000] | Standard |
| Domestic or international donation with one risk Higher Risk Factor (other than potential sanctions risk for which see below) | HKD [25,000] | Standard |
| Multiple Higher Risk Factors and/or potential sanctions or PEP issue (see section 5.5(b) and (c)) | Any | Enhanced |
| High value donation + no Higher Risk Factor | HKD [120,000] | Enhanced |

## [NGO] will not as a matter of usual practice undertake due diligence on donations below the threshold set out in section 5.2(a) given the generally low risk of such smaller donations, as well as the impracticality of identifying the identity of small donors (e.g. street collections, charity boxes).

### No anonymous donations of over HKD [20,000] will be accepted without the approval of [NGO] senior leadership.

## The due diligence process should be undertaken prior to or otherwise as soon as possible on acceptance of a donation from a new donor.

## Standard Due Diligence

### Step 1: Identification and verification

#### For each donor on whom due diligence is required, [NGO] must identify the donor (i.e. collect basic identity information) and verify that identity (i.e. check that the donor is who they say they are) by reference to official/government issued documents (e.g. passport, national identity card, driving license).

#### Individual donors: [NGO] should obtain and verify the individual’s full name, date of birth, nationality, identity card number/travel document number, and current residential address. If it is not possible to meet the individual in person, additional measures should be taken to verify identity (e.g. video conference). Refer to **Appendix B** for more information.

#### Corporate or Institutional Donors: [NGO] should collect and verify the information set out in **Appendix B** for such donor types. [NGO] should also consider the business/industry sector in which the corporate/institutional donor is involved. Specifically, the NGO should review whether that sector is associated with a higher risk of ML (e.g. cryptocurrency platforms, cash-intensive business such as restaurants and other hospitality services, etc.), in addition to whether [NGO] is comfortable being associated with that business/industry sector from a reputation perspective.

### Step 2: Name screening

#### [NGO] should undertake a reasonable search of publicly available information (e.g. internet and media sources) to identify any negative news and/or other information which would increase the ML/TF or reputational risk of dealing with the potential donor. Examples of such information include reports of involvement in criminal activity (including money laundering, terrorist financing, corruption, fraud, etc), enforcement actions by regulatory entities, court judgements, or any other information which raises the risk that the funds are the proceeds of criminal activity and/or that [NGO] could potentially suffer reputational damage from its proposed association with the donor.

##### Targeted searches: the donor’s name should be searched alongside search terms intended to easily identify relevant news. Such search terms include (but are not limited to) the following: allegation, accusation, bribe, fraud, crime, corruption, money launder, terrorism, sanctions, bankrupt, embezzle, political.

#### In addition to the “negative news” screening, searches should also be done to determine whether any donor or Related Individual (see sub-section (iv) below) is or has a material family or business connection to a Politically Exposed Person (“**PEP**”). A PEP is (a) an individual who currently holds or has held a prominent public role in or outside of Hong Kong, (b) a close family member of an individual falling under (a), or (c) a close associate of an individual falling under (a) (e.g. business partner, financial advisor). Given the increased risk of corruption associated with PEPs, [NGO] is required to treat any PEP donors as a “high risk” under section ‎5.6.

##### Examples of PEPs include but, are not limited to, heads of state/government; senior politicians (e.g. cabinet officials, members of the legislature); senior government, judicial or military officials; senior executives of state-owned entities; and important political party officials.

##### Individuals who hold a prominent role in international or regional organizations (e.g. the United Nations, World Bank, International Monetary Fund, European Union), as well as their close family members and close associates, should also be considered PEPs.

##### While there is no single database of global PEPs, prominent political positions should generally be revealed during the name screening searches referenced above. A targeted search using terms such as “political” and “public official” alongside the donor’s name should also be run.

#### Donors and Related Individuals should also be screened against lists of individuals and entities subject to economic sanctions and/or suspected to be involved in terrorist activities.

##### Sanctions imposed by the Security Council of the United Nations (UN) apply in Hong Kong.[[6]](#footnote-7) Information on those sanctions can be accessed on the Hong Kong Companies Registry website[[7]](#footnote-8). A searchable version of the “UN Security Council Consolidated List’ is available on the UN’s website – link in footnote.[[8]](#footnote-9)

##### It is also advisable to review the US, EU and UK lists of sanctions. Although not directly applicable, accepting donations from individuals or entities on those lists could cause material issues for [NGO], including potential problems with financial institutions.[[9]](#footnote-10) See footnote for links to searchable versions of those lists.[[10]](#footnote-11)

##### A true match with a name on any of the lists referenced in sub-sections (A) or (B) above **must be escalated immediately to the Compliance Officer (CO)** (see section 9 for more information). If it is decided to accept the donation, it must be subject to Enhanced Due Diligence (as described in section 5.6 below). Note that all of these lists are continuously updated so [NGO] should ensure that it is using the most recent list when conducting its searches.

#### The above searches should be conducted on the actual donor and any Related Individuals. “**Related individuals**” include:

##### For corporate or institutional donors: beneficial owners and directors;

##### Individual donors: the individual’s direct family members (e.g. spouse, parents, adult children), if known.

### Step 3 - Country Risk

#### [NGO] should consider whether the country of which the donor is a citizen and/or resident is associated with high levels of organized crime, corruption, inadequate systems to prevent and detect ML/TF, and/or economic sanctions. If the country in question is determined to be higher risk in this regard, then the donation **must be escalated immediately to the CO** and enhanced due diligence undertaken.

#### [NGO] should consult the following resources (amongst others) in relation to country risk:

##### Financial Action Task Force (FATF) List of High Risk and Monitored Jurisdictions (updated annually) – see link in footnote.[[11]](#footnote-12)

##### Transparency International’s Corruption Perceptions Index (updated annually) – see link in footnote.[[12]](#footnote-13)

##### List of countries subject to economic sanctions by UN, US, EU and UK – see links in footnote.[[13]](#footnote-14)

##### Basel AML Index – see link in footnote.[[14]](#footnote-15)

## Enhanced Due Diligence for Higher Risk Situations

### [NGO] Individuals must escalate to the CO any potential donor that makes a donation equal to or in excess of HKD [120,000], and/or which presents a higher risk of ML/TF, either through the existence of multiple Higher Risk Factors and/or the presence of sanctions or PEP risk. Where a higher risk situation exists, the CO will advise what additional measures or forms of enhanced due diligence should be applied. This may include:

#### obtaining additional information on the donor (e.g. professional background/CV; reference from a bank or other regulated professional);

#### meeting the donor in person; and/or

#### obtaining additional information on the donor’s source of wealth (i.e. how they earned/acquired their wealth) – e.g. bank statements, audited financial accounts.

### No donations should be accepted by [NGO] where material high-risk factors are present and cannot be mitigated. The approval of the [CO or leadership body - *adapt as needed*] of [NGO] should be obtained to commence or continue any such relationship.

## Ongoing monitoring

### [NGO] should ensure that the due diligence on its donors is regularly reviewed and kept up to date. A risk-based approach should be applied in this regard, meaning that the due diligence relating to the higher risk donors (i.e. those falling under section 5.6 above) should be reviewed more frequently (e.g. on an annual basis) than that of the lower risk donors.

# Beneficiary Due Diligence

## Beneficiary risk

### To the extent that [NGO] distributes cash or other forms of financial support directly to individuals or entities who meet its eligibility requirements (“Beneficiaries”), it is important that [NGO] takes reasonable steps to ensure that any funds so provided are used in accordance with [NGO]’s objectives as set out in the [NGO’s governing document] and not for illicit purposes. These steps will include undertaking risk-based due diligence on the Beneficiary, in addition to reasonable checks on the end-use of the donations. If financial support is provided by [NGO] through a third party/partner organization, reasonable due diligence should be carried out on that organization as well.

### [It is [NGO]’s policy to only donate money to [individuals] [other NGOs].] – *adapt or delete as required*

## Due diligence measures as set out in section ‎5.5 above, as well as a review of the Higher Risk Factors in Appendix A, should be conducted on potential Beneficiaries before the provision of any direct financial assistance to verify that the individual:

### meets [NGO]’s eligibility requirements; and

### does not present a ML/TF or reputational risk to [NGO].

## [NGO’s leadership/governing body] must ensure that [NGO]’s funds are used by the Beneficiaries in accordance with the [governing document/objectives] of [NGO]. In order to fulfil that duty, [NGO] will conduct reasonable and proportionate follow-up monitoring on Beneficiaries after any such financial assistance is provided. This monitoring should include the following (note that this is not an exhaustive list):

### Maintain an audit trail evidencing that the movement of funds from [NGO] to the Beneficiary;

### Ensure that payment from [NGO] to Beneficiary is made to a bank account in the Beneficiary’s name;

### Require the Beneficiary to submit receipts and invoices evidencing their use of the [NGO] funds; and

### Hold in person update meetings with Beneficiaries at regular intervals to assess progress.

# Partner due diligence

## To the extent that [NGO] works with partner charities or organizations in furtherance of [NGO]’s objectives, reasonable due diligence should be carried out on those entities as appropriate so as to check that that partner is bona fide and properly managed, as well as to mitigate the risk of inadvertently working with fraudulent, terrorist or otherwise criminal organizations.

## A risk-based approach to due diligence should also be applied to reviewing partner charities/NGOs.

### Higher risk partners: Where [NGO] is entering into a significant relationship with a partner organization (in the context of [NGO]’s overall activities/profile), the partner has some higher risk characteristics (e.g. from a higher risk country, or is connected with PEPs), and/or the partner will be handling funds on behalf of [NGO], [NGO] should at a minimum conduct the checks and screening described in section 5.5. Where significant funding is likely to be handled by the partner, the additional checks described in section 5.6 above, in addition to other forms of financial due diligence, should be considered. Essentially, the higher the risk, the more extensive the checks should be before agreeing to work with the partner.

### If the work with the partner organization is not substantial or otherwise high risk, [NGO] should at a minimum ensure that the partner entity is bona fide/exists (including checking tax exempt status under section 88 of the Inland Revenue Ordinance for Hong Kong entities, and if the partner is in a jurisdiction which regulates charities/NGOs, the relevant register should be reviewed to check the entity’s inclusion/status); identify the key people at the partner organization; and undertake name screening as described in section 5 on the partner entity and the key individuals. [NGO] should also review the list of Higher Risk Factors in Appendix A in the context of the partner’s profile/business.

## As part of general anti-fraud measures, [NGO] should also at a minimum:

### undertake name screening (as set out in section 5) and other forms of background checks (e.g. reference checks) of all new [NGO] Individuals as part of the on-boarding process; and

### complete at least standard due diligence (as set out in section 5) on suppliers with whom [NGO] has a material (in terms of monetary value or importance to [NGO] operations) and/or continuing (i.e. not a “one-off”) contract.

# Third party transactions

## “Third party transactions” refer to transactions where [NGO] receives funds from, or is asked to remit funds to, a third party other than the donor, beneficiary or partner on whom [NGO] has undertaken its due diligence. Examples include:

### [NGO] is requested by a beneficiary or partner to whom it has agreed to provide funds to instead remit those funds to a third party; or

### In the case of a donation, [NGO] unexpectedly receives funds from a third party payor/account instead of directly from the donor.

## The [NGO] should not accept or agree to third party transactions other than in exceptional circumstances where [NGO] is satisfied that:

### Enhanced due diligence (as set out in section 5.6) on the third party payor or payee presents no material ML or TF risk;

### The relationship between the donor, beneficiary or partner and the third party payor/payee is transparent, credible and documented;

### There is a legitimate, credible and documented explanation for the involvement of the third party; and

### [NGO]’s CO/MLRO (as defined in Section 9 below) approves the third party transaction.

## If [NGO] cannot satisfy itself that the third party transaction is acceptable following the steps described in section 8.2, [NGO] must decline the transaction and consider its reporting obligations under section 10.

# Compliance Officer/Money Laundering Reporting Officer

## [NGO]’s designated compliance officer (“**CO**”) is [x].[[15]](#footnote-16)

## The principal function of the CO is to act as the focal point within [NGO] for the oversight of all activities relating to the prevention and detection of ML/TF and to provide support and guidance to [NGO] Individuals with the objective of ensuring that ML/TF risks are adequately managed. In particular, the CO should assume responsibility for developing and/or continuously reviewing [NGO]’s AML compliance framework (including this Policy) to ensure it remains up-to-date, effective and consistent with current statutory and regulatory requirements, as well as reflecting the risk profile of [NGO]’s donor/beneficiary base.

## [NGO]’s CO is also its designated money laundering reporting officer (“**MLRO**”). As set out in section 10 of this Policy, any [NGO] Individual having knowledge or suspicion of money laundering must disclose that development to the MLRO.

## The MLRO should play an active role in the identification and reporting of suspicious transactions. Principal functions include:

### reviewing all internal reports from [NGO] Individuals and, in light of all available relevant information, determining whether or not it is necessary to make a report to the Joint Financial Intelligence Unit (“**JFIU**”);

### maintaining all records related to such internal reviews;

### providing guidance on how to avoid “tipping off” if any disclosure is made; and

### acting as the main point of contact with the JFIU, law enforcement, and any other competent authorities in relation to ML/TF issues.

# Suspicious Transaction Reports

## Statutory framework

### As referenced in Section 3, it is an offence under Hong Kong law for any person in Hong Kong to fail to disclose knowledge or suspicion of money laundering or terrorist financing. Failure to report such knowledge or suspicion under the Hong Kong statutory framework can be punished with imprisonment and/or a significant monetary fine.

### For a person to have the requisite knowledge or suspicion, they do not need to know the nature of the criminal activity underlying the money laundering, or that the funds themselves definitely arose from the criminal offence.

### The disclosure of knowledge or suspicion of ML/TF is referred to as a suspicious transaction report (“**STR**”). The filing of an STR with the JFIU provides [NGO] with a statutory defense to the offence of ML/TF in respect of the acts disclosed in the report, provided: (a) the report is made before [NGO] undertakes the disclosed acts and the acts are undertaken with the consent of the JFIU; or (b) the report is made after [NGO] has performed the disclosed acts, and the report is made on [NGO]’s own initiative and as soon as it is reasonable for [NGO] to do so.

### Once an [NGO] Individual has reported their suspicion relating to a potential or actual donor/beneficiary (or related transaction) to the MLRO in accordance with the procedure described in this Policy for the making of such disclosures, the individual has fully satisfied their own personal statutory obligation to report such suspicions.

### It is also a criminal offence (“tipping off”) for an [NGO] Individual to reveal to any person information which might prejudice an investigation. For example, if an STR (internal within [NGO] or external to the JFIU) is made about a donor and the donor is told that a report has been made, any investigation into the donor’s activities by law enforcement would potentially be prejudiced and the “tipping off” offence would be committed.

### The NSL also includes an obligation that requires an individual to make a report to law enforcement if they “know” or “suspect” that any property is Offence related property.[[16]](#footnote-17) Scenarios which would trigger the disclosure obligation include (but are not limited to) an NGO learning that a person has been arrested for/ charged for an Offence; and/or an NGO having knowledge or suspicion that funds/assets are Offence related property after receiving information from law enforcement agencies. The procedures for making STRs described in this Section will also apply to reports made under the NSL.

##  [NGO] STR Procedure

### If any information or other matter comes to the attention of any [NGO] Individual which gives rise to knowledge or suspicion that another person is involved in ML/TF activities, or if the [NGO] Individual has an unresolved concern about any unusual donation or circumstance, the [NGO] Individual must discuss the matter with the MLRO as soon as possible.

### The MLRO must acknowledge receipt of the “report” and remind the [NGO] Individual about the obligation regarding tipping off. The tipping-off provision includes circumstances where a suspicion has been raised internally, but has not yet been reported to the JFIU. Once a report has been made to the MLRO, no communication concerning the reported matter may be made with, or further enquiries made of, the donor, beneficiary or any other party concerned without the MLRO’s prior written approval.

### It is the responsibility of the MLRO to review the information and to make a decision as to whether the suspicion is justified. In doing so, the MLRO should consider the matter in the light of all other relevant information and make a decision as to whether any concerns remain. If in following this process the MLRO confirms that the circumstances give rise to knowledge or suspicion of ML/TF, the MLRO must report the matter by making an STR to the JFIU.

### The JFIU will send the MLRO a letter acknowledging receipt of the STR. If consent to proceed with a transaction/donation has been requested, then no action should be taken unless and until consent from the JFIU is obtained. Otherwise there is a risk of [NGO] committing the criminal offence of dealing with the proceeds of crime.

### MLRO Recordkeeping

#### If the MLRO determines that no report is required to be made to the JFIU, a copy of the record of the internal report made by the [NGO] Individual and the related discussions should nevertheless be made and filed in the [NGO] JFIU register.

#### The record of all internal reports made to the MLRO should include details of the date the report was made, the names of [NGO] Individuals subsequently handling the report, the results of the assessment, whether the report resulted in a disclosure to the JFIU, and information to allow the papers relevant to the report to be located.

#### The record of all STRs made to the JFIU must include details of the date of the disclosure, the name of the MLRO, and information to allow the papers relevant to the disclosure to be located. This register may be combined with the register of internal reports, if considered appropriate.

# Record Keeping

## [NGO] should retain the original or a scanned copy/photocopy of documents used to identify and verify donors/beneficiaries, in addition to a record of other information (e.g. results of name screening) obtained in the course of completing the due diligence process outlined in this Policy. These records should be kept in relation to all donors, beneficiaries, persons who purport to act on their behalf, other connected parties, and/or any other organizations with whom [NGO] enters into a working relationship.

## All documents and records mentioned in section ‎11.1 should be kept throughout the relationship with the donor/beneficiary and for a period of 7 years after the end of the relationship.

## Records can be retained in paper or electronic form.

# Staff Training

## All [NGO] Individuals must:

### Receive a copy of this Policy and confirm in writing on an annual basis that they have read and understood it; and

### Complete AML training as advised by the CO as soon as possible after the commencement of their work with [NGO].

## Refresher training should be offered to [NGO] Individuals on a regular basis, in particular to those who deal with donors / beneficiaries directly.

Please contact [x], the Compliance Officer at +852 [x] if you have any queries on this Policy.

APPENDIX A

Examples of situations involving donors, beneficiaries and/or partners which may indicate a higher risk for money laundering and/or terrorist financing include (but are not limited to) the following:

###### Donation from known donor but which comes through an unknown party or unusual payment mechanism (e.g. donation made using a large number of fund transfers in small amounts, perhaps to avoid triggering reporting requirements).

###### Unusual or substantial one time donations, or a series of smaller donations or interest-free loans, from a source that cannot be adequately identified.

###### [NGO] is asked by a donor to engage in specific work and/or deliver work product for the exclusive use of the donor, particularly in cases where that work is outside [NGO]’s area of focus.

###### [NGO] is requested by a beneficiary or partner to whom it intends to provide funds to instead remit those funds to a third party.

###### In the case of a donation from a donor on whom client due diligence has been undertaken, [NGO] unexpectedly receives funds from a third party payor/account instead of directly from the donor.

###### [NGO] is asked to act as a conduit for passing a donation to second individual or body, which may or may not be another charity.

###### Conditions are attached to a donation such that the [NGO] is effectively only serving as a vehicle for transferring funds from one source to another without the charity serving any other role.

###### A donation is provided to the [NGO] for a defined period of time during which the charity can retain any interest earned; however, the principal sum is required to be returned at the end of the defined period.

###### Same as the preceding example but the donation is in a foreign currency and the principal sum is to be returned in a different currency.

###### A donation is conditional on specific individuals or organizations being used to do work for the [NGO] in cases where the [NGO]’s leadership have concerns about such individuals or organizations.

###### [NGO] is asked to provide services or benefits on favorable terms to the donor or a person nominated by the donor.

###### A donor, partner or beneficiary who is unusually secretive or reluctant to provide information for the due diligence or post-donation monitoring process.

###### Donor who is using a network of trusts and/or shell companies through which to make its donation.

###### The donor, partner or beneficiary is a citizen or resident of a high risk country, and/or the donation is being sent from a bank account in a high risk country.

###### The source of wealth for a donor is unclear and/or not commensurate with the donor’s known background or income.

###### The donor or partner is or is closely connected to a PEP; this would be particularly high risk if the underlying PEP position is connected with a high risk country for corruption.

###### The donor, partner or beneficiary is or is closely connected an individual or entity on a sanctions list.

###### The donor, partner or beneficiary is associated with activities which could be considered to fall under the NSL.

###### The donor’s source of wealth is derived from/closely associated with an industry sector which is higher risk for ML (e.g. cryptocurrency platforms, cash-intensive businesses such as restaurant or other hospitality services).

###### The donor, partner or beneficiary is the subject of material negative news – e.g. arising from legal, regulatory or enforcement actions; allegations of fraud, money laundering, corruption or other crimes; unscrupulous business practices.

APPENDIX B

1. Standard Due Diligence (individual)
	1. Identify: full name, date of birth, nationality, identity card number/travel document number, and proof of residential address.
	2. Verify the information collected in (a) by viewing original copy of the documents referenced below. If unable to view original copy, consider requesting copies of the documents in question which have been certified as “true copies” by a qualified solicitor, accountant or other similar regulated professional.

|  |  |
| --- | --- |
| **Individual** | **Documents required**  |
| Hong Kong Resident  | Hong Kong Identification CardProof of residential address from an official source (e.g. utility bill, bank statement, tax bill, official government correspondence, etc) – dated within the last three months.  |
| Non-Hong Kong Resident | Current/valid passport or national identification cardProof of residential address from an official source (e.g. utility bill, bank statement, tax bill, official government correspondence, etc) – dated within the last three months.  |

### No form of identification can be fully guaranteed as genuine or representing correct identity. [NGO] Individuals should recognize that some types of documents are more easily forged than others. If suspicions are raised in relation to any document offered, [NGO] Individuals should take whatever practical and proportionate steps that are available to establish whether the document offered is genuine, or has been reported as lost or stolen. This may include searching publicly available information, approaching relevant authorities or requesting corroboratory evidence from the donor. Where suspicion cannot be eliminated, the document should not be accepted and consideration should be given to making a report to the authorities as set out in section 10.

1. Standard Due Diligence: Corporate and Institutional Donors
	1. Identify:
		1. Full legal name and trading name (if different);
		2. Place and date of incorporation;
		3. Corporate and business registration number;
		4. Registered address and primary business address (if different);
		5. Nature/type of business; and
		6. If privately owned (i.e. not publicly listed):
			1. Full names of Directors
			2. Full names of any individual shareholders owning more than 25% of the entity (“beneficial owners”).
	2. Verification:
		1. The information collected in 2(a) above should be verified to the extent possible using publicly available resources, including the Hong Kong Company Registry (for Hong Kong-incorporated companies).
		2. The verification procedures for individuals as set out in the first section of this Appendix B should be undertaken on individual shareholders owning or controlling more than 25%. If there are no such shareholders, then the identity of two directors should be verified.
			1. The verification of individual shareholders is not needed where the donor is listed on the Hong Kong or other equivalent stock exchange, or where the donor is regulated by a Hong Kong financial regulator (e.g. the Securities and Futures Commission, Hong Kong Monetary Association). In such cases, [NGO] should retain evidence of such listing or regulation for its records.
1. While UNATMO expressly excludes protest, industrial action and other forms of advocacy/dissent from its definition of “terrorist act,” the NSL notably does not include such an exclusion. [↑](#footnote-ref-2)
2. https://www.cr.gov.hk/en/publications/docs/hkrisk\_assessment\_report-e.pdf [↑](#footnote-ref-3)
3. <https://www.nd.gov.hk/pdf/guideline_e_20180929.pdf> [↑](#footnote-ref-4)
4. Drafting note: note that the thresholds in this and the subsequent section are suggestions only and can be lowered or raised depending on [NGO’]s risk profile, risk appetite, profile of donors, and resource constraints. Re the HKD 120K threshold for enhanced due diligence, that was chosen as it is the threshold in the Hong Kong ML statute over which due diligence is required for transactions with “one off” customers (i.e. no underlying business relationship). [↑](#footnote-ref-5)
5. Note [NGO] should be guided by a risk-based approach in this scenario - the more severe the risk factor in question, the more extensive the due diligence should be. For example, if the donation comes from a citizen of a country subject to sanctions (e.g. Iran), that should be treated as a much more serious risk than if a donation comes from an unsanctioned higher risk country (e.g. Brazil). [↑](#footnote-ref-6)
6. United Nations Sanctions Ordinance (Cap. 537). [↑](#footnote-ref-7)
7. <https://www.cr.gov.hk/en/amlctf/lists.htm> [↑](#footnote-ref-8)
8. <https://www.un.org/securitycouncil/content/un-sc-consolidated-list> [↑](#footnote-ref-9)
9. If an individual subject to US sanctions related to Hong Kong (i.e. the Hong Kong Autonomy Act) proposes to make a material donation to [NGO], then depending on the circumstances of the donation and the international footprint/connections of [NGO] at that time, [NGO] will consider obtaining specialist legal advice on the issue. [↑](#footnote-ref-10)
10. US sanctions- Office of Foreign Assets Control “Specially Designated Nationals and Blocked Persons List”: <https://sanctionssearch.ofac.treas.gov/>; EU sanctions/restrictive measures- “Consolidated list of persons, groups and entities subject to EU financial sanctions: <https://ec.europa.eu/info/business-economy-euro/banking-and-finance/international-relations/restrictive-measures-sanctions_en#list> ; and UK sanctions - Office for Financial Sanctions (OFSI) List of UK Sanctions: <https://www.gov.uk/government/publications/the-uk-sanctions-list> [↑](#footnote-ref-11)
11. <https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)>. [↑](#footnote-ref-12)
12. <https://www.transparency.org/en/cpi> [↑](#footnote-ref-13)
13. For the UN, please refer to section 5.5(b)(iii) above. US (<https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information> ); EU (<https://sanctionsmap.eu/#/main> ); UK (<https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases> ). [↑](#footnote-ref-14)
14. [Basel AML Index | Basel Institute on Governance (baselgovernance.org)](https://baselgovernance.org/basel-aml-index) [↑](#footnote-ref-15)
15. Drafting note: CO can hold other roles within the NGO. While CO and MLRO roles will usually be held by same person, that does not have to be the case. [↑](#footnote-ref-16)
16. Refer to definition in section 3.1(e) above. [↑](#footnote-ref-17)