TZU CHI FOUNDATION

ANTI-MONEY LAUDERING (AML) AND COUNTER TERRORISM FINANCING (CTF) POLICIES

TABLE OF CONTENTS

1 INTRODUCTION, SCOPE AND OBJECTIVES

Non-Profit Organisations ("NPO") traditionally enjoy a high and strong level of trust by society at large. In the Fourth Round Mutual Evaluation Report on Anti-Money Laundering and Counter-Terrorist Financing Measures – Malaysia published by the FATF, the FATF has identified that there are gaps in administrative sanctions for compliance failures with obligations on NPOs and gaps in explicit record keeping requirements with regards to the NPOs.

In 2015, religious, charitable and political NPOs account for about 40% of NPOs are considered a high-risk Terrorism Financing area in the National Risk Assessment (NRA). The NRA indicated that approximately 1000 of a total of more than 47,000 NPOs' accounts are used for majority of international financial transactions and activities.

The Foundation deals with the operation and management of charitable missions in both local and international level, such as educational sponsorship, medical support and humanitarian aid mission in disastrous events. The Foundation believes that a sound and proper system shall be put in place and shall be maintained and updated from time to time because the Foundation as a registered charitable organisation in Malaysia, it solicits and receives donations from its members, volunteers and society at large.

To gain trust and confidence from the donors will definitely help to reflect the integrity value practiced by the Foundation. To prevent any breach in the integrity of the Foundation which will result in jeopardising the charitable missions of the Foundation, hence donors losing confidence in the Foundation, the system employed by the Foundation shall be robust and always in compliance with the relevant laws and regulations that will prevent the Foundation from being used by criminals or unscrupulous individuals or entities to commit harm or losses to not only innocent donors, but also to the government, society and the world at large.

In this regard, processes are emplaced to prevent the Foundation's services or channels from being used for money-laundering and terrorist-financing activities as well as safe-guarding donors' personal information and banking data. Control measures are also being emplaced to identify, assess, mitigate, monitor and report such risks. They include conducting due diligence on all relevant personnel, including the office bearers, personnel involved in management affairs, volunteers and donors. Promoting greater transparency will protect the integrity of the financial system and strengthen incentives to prevent their abuse for illegal activities.

The Foundation demonstrates its full commitment and support to high standards of compliance with the AML & CFT requirements by establishing a comprehensive policy, procedures, processes and systems for the prevention and detection of money laundering and terrorist financing activities and shall ensure compliance with the requirements of the Anti-Money Laundering and Anti-Terrorism Financing Act 2001 (AMLATFA 2001) at all times. This AML & CFT Guidelines ("**Guidelines**") provides standard and specific guidance for of compliance with the AML & CFT requirements.

2 RISK-BASED APPROACH

A risk-based approach should be adopted as aligned to the Financial Action Task Force ("**FATF**") recommendation to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identifies and that effort is directed proportionately with appropriate flexibility to effectively manage areas with real risks. The Foundation has summarised a risk-based approach to AML as covering:

- Risk-identification and assessment
- Risk mitigation
- Risk monitoring
- Documentation

Reasonable steps must be taken to identify and strengthen any weak links in the AML/CTF controls and processes with proportionate time and recourse focused on strengthening the weak links. The management of the Foundation has been tasked to ensure that risks are managed appropriately.

Risk-identification and assessment

The risk assessment process is to identify and determine the inherent risks i.e. before any controls being applied, on money laundering / terrorism financing / financial and economic sanctions that the operation is exposed to, thus allowing the design of appropriate mitigating controls and strategy.

The level of inherent risks is determined by:

- The geographical location of operation (country risk);
- The services provided (product risk);
- The services delivery channels (distribution risk), including consideration of any outsourced services;
- The donor base (donation risk); and
- The financial sanctions regime (financial sanction risk).

The risk assessment is not a one-off process by but a continual effort. The Foundation must assess the different types of inherent risks regularly, as well as when changed circumstances arise. Any risk identified during the assessment shall be highlighted and additional controls or assurance work identified can be incorporated.

Risk mitigation

Controls must be designed and implemented to mitigate the inherent money laundering or terrorism financing or financial and economic sanctions risks identified. It is understood that no control can completely eliminate the risks therefore the residual risks need to be assessed in order for the Foundation to determine if they are content with the risk exposure or to implement additional controls to further mitigate the risks. The mitigating controls should be tested on a periodic basis to ensure effectiveness.

Risk monitoring

Whenever there is a change in local AML or CTF laws or regulations, the Foundation must conduct gap analysis promptly to identify if there is any disparity between the current practice and the new requirements. Action plans need to be formulated accordingly and as appropriate.

Documenting the risk-based strategy

The risk based approach, including but not limited to the following, must be documented in order to demonstrate to the Foundation or the relevant regulators / authorities:

- Supporting documents on the risk position and assessment including rationale and justification;
- Risk assessment approval note / evidence;
- Application, monitoring and testing of controls; and
- Data, statistic and reporting.

3 DONOR SOLICITATION / ACQUISITION, DONOR DUE DILIGENCE AND TRANSACTION MONITORING

Due diligence (including sanctions screening approach) on donors should be carried out according to the mitigating strategy outlined in the risk assessment. For reference purpose, such method is known as the Customer Due Diligence or the Know Your Customer (KYC) policy and often to be used interchangeably. For the purpose of the Foundation, the terminology of "Customer" shall mean and be referred as the "Donor" at all material times. The Donor shall mean any person regardless of his or her identity as a member or non-member, that willingly or voluntarily contribute, donate and/or giving out his or her form of contributions that monies' worth such as cash, properties or assets to the Foundation for the purpose to support the Foundation's charitable missions.

Customer Due Diligence ("**CDD**")

Generally, the donors base of the Foundation is divided into members and non-members. Members are usually the volunteers that registered with the Foundation that assist the Foundation to execute and carry out charitable missions such as in the area of medical, education, charity and cultural supports. The Foundation keeps all the donation records from all members.

Non-members are normally the public at large where they are not registered members with the Foundation and the Foundation has no personal particulars of such non-members. More often than not, non-members may choose to donate anonymously by way of offline physical cash into donation boxes or via members.

As the methods of donation comprising of both offline and online, the appropriate CDD measures should be in place.

CDD is carried out for the purpose of verifying the donor's identity and understanding the nature and purpose of the relationship, so that the donation can have more and reasonable assurance that:

- The Foundation knows from whom it received the donation;
- The donation given are appropriate to be received for;
- The Foundation is able to form a view on the expected behaviour and activities for such donors; and
- The Foundation is not engaging with any sanctioned targets.

A) Donor onboarding

CDD should be conducted prior to or as soon as possible after entering into a relationship with a donor. The Foundation's policies in relation to entering into a new relationship with a donor must be observed at all times, for example, gathering and collecting donor's information from the CDD process shall be completely and correctly recorded for the purpose of proper risk rating / scoring, screening and

monitoring. Quality assurance check on data entry and data integrity should be performed.

B) Prohibitions

The Foundation will not establish relationships with:

- Donors in obviously fictitious names;
- Shell banks; or
- Offshore entities except those in the Federal Territory of Labuan.

C) Ongoing CDD and Re-screening

CDD information should be kept up-to-date and refreshed whenever practical. CDD information of high risk donors should be refreshed at least annually. Donors should undergo sanctions re-screening on a regular basis even in the absence of transactions, as sanctions re-screening restrictions and other watch-lists are updated on an ongoing basis. Donor's risk must be re-assessed if there has been any change to the profile or circumstances.

Customer Risk Rating, High Risk Customer ("**HRC**") and Enhanced Due Diligence ("**EDD**")

A) Customer risk rating

Customer risk rating is determined according to the risk scoring system adopted by the Foundation using the risk based approach. Risk factors shall be considered solely, or in combination, or with a monetary threshold applied to derive the customer risk classification system.

B) Qualifying threshold for customer risk classification

It is recognised that transactions of low monetary value generally have lower money laundering risk. For the sole purpose of receiving donation, the qualifying threshold adopted by the Foundation is consistent with the proposed cash transaction limited to be imposed by the Central Bank of Malaysia which is RM25,000.00.

Any donation or transaction with a donor shall subject to this qualifying threshold and if a transaction falls below than the qualifying threshold, it will be exempted from the risk classification process and the donor will be considered as regular risk. However, risk classification process must be applied on all donors classified under politically exposed person ("**PEP**"), special interest person ("**SIP**")/special interest entity ("**SIE**") and relatives and close associates ("**RCA**") status and all shell companies especially those companies incorporated in 'tax heaven' countries regardless of whether their business proposal exceeding the qualifying threshold or not.

Note that ongoing transaction monitoring on the customer activity will need to be conducted regardless of the customer risk rating to detect any unusual transaction

or pattern such as high volume of multiple low value transactions entered within a short period of time.

C) Customer risk classification

When risk assessing a donor, a predefined set of risk attributes shall be considered together in a weighted manner to determine the overall risk level of the customer. A risk scoring mechanism shall be implemented to minimise subjectivity and maximise consistency when risk classifying customers; each risk attribute will be given a score and the total risk score will indicate the risk level of the donor.

For individual, the following is the minimum set of risk attributes to be considered/implemented:

- Donation solicitation channels shall be risk categorised e.g. non-members referral should be of higher risk than donors referred by members of the Foundation;
- Monetary value – an appropriate threshold shall be set to indicate large transaction value which warrants more attention;
- Occupation – a list of high risk occupations shall be defined;
- Residency – a list of risk jurisdictions shall be defined, of which should include countries identified as high risk by the European Commission, United Nations, those countries not considered to be compliant with Financial Action Task Force ("**FAFT**") recommendations and local regulator published high risk countries. The Foundation should also consider tax heaven countries when defining the list of high risk jurisdictions.
- Nationality – the same list of high risk jurisdiction as for the residency shall be used but the relative risk score for nationality match may be lower due to smaller risk compared with Residency;
- Donor profile – the donor shall be first screened against sanctions, PEP, SIP and RCA lists available and a relative score shall be defined for each type of match if the donor intends to donate beyond the qualifying threshold; and
- Other money laundering risk factors:
    - Aggregate transactions for the same donor – similar to the monetary value of the single transaction, an appropriate threshold shall be set to indicate larger aggregate transaction which warrants more attention;
    - Any previous suspicious activities by the same donor – any previously confirmed suspicious activity, including those filed to local authority or enforcement body shall effect the donor as possibly high risk;
    - Affordability of the transaction – the donation amount shall be assessed against the earning power and wealth of the donor to determine if it is economically sensible; and
    - Any other indication of higher risk – any unusual behaviour or activity noted shall form part of the assessment.

For corporate donor, the following is the minimum set of risk attributes to be considered/implemented:

- Donation solicitation channels shall be risk categorised e.g. non-members referral should be of higher risk than donors referred by members of the Foundation;
- Monetary value – an appropriate threshold shall be set to indicate large transaction value which warrants more attention;
- Business sector – a list of high risk business sector shall be defined;
- Operating country – a list of risk jurisdictions shall be defined, of which should include countries identified as high risk by the European Commission, United Nations, those countries not considered to be compliant with FAFT recommendations and local regulator published high risk countries. The Foundation should also consider tax heaven countries when defining the list of high risk jurisdictions.
- Registration country – the same list of high risk jurisdiction as for the operating country shall be used but the relative risk score for registration country match may be lower due to smaller risk compared with Operating country;
- Donor profile – the donor shall be screened against sanctions and SIE lists available and the beneficial owners shall be screened to check for any corresponding PEP/SIP/RCA, a relative score shall be defined for each type of match if the donor intends to donate beyond the qualifying threshold; and
- Other money laundering risk factors:
    - Aggregate transactions for the same donor – similar to the monetary value of the single transaction, an appropriate threshold shall be set to indicate larger aggregate transaction which warrants more attention;
    - Any previous suspicious activities by the same donor – any previously confirmed suspicious activity, including those filed to local authority or enforcement body shall effect the donor as possibly high risk;
    - Affordability of the transaction – the donation amount shall be assessed against the earning power and wealth of the donor to determine if it is economically sensible;
    - Beneficial ownership structure – attention shall be given to unlisted companies having complex and unclear beneficial ownership structure which are more prone to be utilised for financial crime and a higher risk score shall be defined for such; and
    - Any other indication of higher risk – any unusual behaviour or activity noted shall form part of the assessment.

D) <u>Material transaction cases as high risk</u>

Transactions or donation involving material monetary value inherently pose higher money laundering risk as these are more prone to be utilised as vehicles for money laundering. In order to minimise this risk, donor with material transaction cases must be treated as high risk customers and enhanced due diligence measures must be applied to assess the risk involved before making an informed decision on accepting/retaining or rejecting the donor's donation.

E) <u>Enhanced Due Diligence requirements</u>

Enhanced Due Diligence must be applied when engaging high risk donors, which involves obtaining additional information and/or documents to verify the donor and

the beneficial donor's identity. This will include obtaining the following items where applicable:

- More details on the ownership and control structure of the corporate donors;
- More details on the nature and details of the business / occupation / employment;
- A record of changes of address;
- Information on the immediate source of fund;
- The expected origin of the funds to be used in the transaction;
- The ongoing source(s) of wealth or income;
- More details on the activity from which the funds have ultimately derived;
- The purpose and reason for establishing the business transaction;
- The various relationships between signatories and underlying beneficial owners;
- The anticipated level and nature of the activity that is to be undertaken throughout the relationship;
- Copies (should be certified true copies where possible or with the original sighted and confirmed) of recent and current financial statements of corporate donors; and
- Documentary proof (should be original, sighted and confirmed or certified true copies where possible) of source of income / wealth e.g. current bank statements demonstrating source of monies or regular income / recent and current audited financial statements for corporate donors.

Enhanced Due Diligence on new high risk donors identified during take on shall be performed prior to acceptance. Note that high risk donors can also be identified during the course of donation (due to changes in circumstances or profile). Enhanced Due Diligence must be applied wherever a new high risk donor from the existing donor database is identified.

<u>Exception cases</u>

It is recognised that some donors may be unable to provide sensitive and non-public information on financial standings, a risk based holistic approach on Enhanced Due Diligence can be carried out when such situation arises.

Best effort shall be put in place to obtain the information and supporting documents recommended by the money laundering reporting officer of the Foundation ("**Compliance Officer**"). If the donor is unable to provide this information or documentation, the following procedures can be followed for these exception cases:

- Document that Enhanced Due Diligence has been attempted to obtain with reason clearly documented for failure to fulfil these requirements; and
- Conduct further research and compile information based on all the items below to provide a holistic view of the donor relationship for risk assessment. The information gathered must be documented clearly as part of the whole case for review and consideration. Any item or supporting document which cannot be achieved, with the reason for failure, also needs to be documented as part of the case:

- Effect face-to-face discussion to ascertain existence of the individual or entity and form a view on their legitimacy;
- Research on the donor background by utilising public and commercial database or engage external professional firm for background check;
- Consider whether the donor introduction channel is trusted and reputable;
- Consider whether reasonable assurance is obtained for any reliance placed on the intermediary for Know Your Customer / Customer Due Diligence / Enhanced Due Diligence of such high risk donor. Additional caution to be exercised when the intermediary is remunerated on a commission basis;
- Access the risk of the source of fund, i.e. where the fund for the donation is from. For cases where bank transfer is the reason, for additional comfort, the rationale should be documented as audit trail.

F) High risk customer approval process

For all donors classified as high risk, either identified during on-boarding or throughout the course of the business relationship, the following process must be triggered:

- Enhanced Due Diligence process shall be triggered;
- Result of the Enhanced Due Diligence to be reviewed and signed off by the Compliance Officer;
- For exception cases, the case must be escalated to the Foundation's office bearers for further review;
- All approvals for the establishment or continuity of the donor with rationale must be clearly documented;
- Log and maintain the donor relationship on the high risk donor register; and
- Conduct special monitoring on the donations or transactions.

G) Removal of high risk donor

Donor risk rating could be lowered throughout the donor life cycle due to changes in circumstances (e.g. residency of donor changed from a high risk jurisdiction to a low risk jurisdiction) and high risk donor can become a normal/low risk donor. In such event, the removal of high risk donor (or lowering of the donor risk rating) needs to be documented with justification and signed off by the Compliance Officer. Subsequently, the particular donor can be un-tagged for special transaction monitoring and excluded from the high risk donor register.

Politically Exposed Persons

PEPs inherently pose higher money laundering risks and warrant more attention, especially when there are also specific concerns on PEPs from regulators and international bodies such as the FAFT. Risk based approach on PEP (including their RCAs) donor handling can be adopted, where PEP can be classified as high risk or low risk donor based on the donor risk classification mechanism.

However, the following process is required for all PEP donor relationship (including those of their RACs) regardless of the risk classification of the donor:

- Review the donor profile and Customer Due Diligence / Enhanced Due Diligence result to access risk;
- The Foundation's money laundering reporting officer's approval for establishing (or continuing) the donor relationship with rationale properly documented;
- Log and maintain the donor relationship on the PEP register;
- Monitor the relationship and trigger high risk donor process should the PEP become a high risk donor; and
- Conduct standard monitoring (for low risk PEPs) or special monitoring (for high risk PEPs) on the donations or transactions.

Collection of money by the Foundation

Money laundering, misappropriation and mishandling of donor's money all count as serious misconduct and may expose the Foundation to undue money laundering as well as fraud risks. To avoid such incidents and better protect the Foundation and the donors, the use of traceable non-cash equivalents directly from the donors as the means of payment channels is recommended e.g. direct bank transfer or credit card remittance.

It is a norm for the Foundation to receive cash donation directly from the donation boxes placed in the premises of the Foundation. Notwithstanding that, the Foundation will monitor any unusual or abnormal amount of donation from time to time.

Transaction Monitoring

Monitoring of donor relationship is required on an on-going basis, where different extent of monitoring should be applied according to the risk profile. High risk donors are to be monitored more frequently and intensively. The Foundation recommends a monitoring frequency of quarterly for standard monitoring as opposed to every month monitoring for special monitoring.

The review process and decision rationale must be clearly documented for all reviewed cases on a suspicious transactions monitoring log. Special monitoring shall only be ceased when the donor is no longer classified as high risk. Where practical, high risk donors should be tagged and any new transactions should be directed to the compliance or anti money laundering unit of the Foundation for clearance before processing any new requests or transactions. Monitoring mechanism, including red flags, should be reviewed and tested annually to ensure effectiveness.

Payment by Foundation

Sanctions screening should be performed on the recipients of funds prior to any pay-out. High risk outward payment such as foreign wire payment requires additional screening to include all parties to the transactions. This includes the remitting/receiving bank and any correspondent bank (if provided). In particular payment in USD should be screened as near to as practically possible the time of payment. No payment should be made to a bank that is 50% or more owned by a sanctioned entity/individual.

With regards to the recipient of funds whom might be listed as targeted person to be assisted under the Foundation's charitable missions including but not limited to single parent, physically or mentally disabled person, the Foundation recommends such person to be registered as a member of the Foundation for profiling purpose. In the event such person refused to register as a member, the Foundation will conduct KYC on such person to obtain his or her personal particulars.

Outsourcing

For outsourcing of any AML related services, the Foundation needs to conduct due diligence and document the assessment on the service provider to ascertain satisfactory AML systems and controls are in place following local regulations. If gap exists between the Foundation's standards and that of the service provider, the Foundation should try to negotiate with the provider to apply the Foundation's standards. Any remaining gaps shall be documented and the risk exposure needs to be considered before establishing the relationship. The Foundation should impose contractual requirement on the service provider to establish and maintain adequate and appropriate AML systems and controls in relation to the outsourced service. Clauses on right of audit and access should be included where possible on the outsourcing agreement, or alternatively, a copy of the service provider's most recent system audit report to be obtained for assurance purpose.

Due diligence on the service provider should include but not limited to the following:

- Understanding (and obtaining reasonable assurance as appropriate) the AML policies, systems, controls and processes in place at the service provider;
- Researching on the service provider for any historic breach of regulations and/or adverse media related to financial crimes;
- Performing sanctions screening on the service provider;
- Assessing the money laundering / terrorist financing / financial and economic sanctions risks for outsourcing the particular service to this provider.

Relationship with outsourced service provider should also be reviewed and the provider re-screening be conducted regularly (annual basis).

Partners

The Foundation should conduct due diligence and document the assessment on partners to ascertain satisfactory AML system and controls are in place following local regulations and Foundation's standards. If gap exists between the Foundation and that of the partner, the Foundation should try to negotiate with the partner to apply the Foundation's standards. Any remaining gaps shall be documented and the risk exposure to be considered before establishing the relationship.

Due diligence on the partner should include but not limited to the following, taking into account the service to be provided by the partner:

- Understanding (and obtaining reasonable assurance as appropriate) the AML policies, systems, controls and processes in place at the partner;

- Researching on the service provider for any historic breach of regulations and/or adverse media related to financial crimes;
- Performing sanctions screening on the partner;
- Assessing the money laundering / terrorist financing / financial and economic sanctions risks for appointing the partner for the particular service; and
- The decision to proceed should be made by the Compliance Officer.

Relationship with the partner should also be reviewed and the provider re-screening be conducted regularly (annual basis).

In order to demonstrate strong commitment and attention on AML / CTF / financial and economic sanctions compliance and to mitigate any potential risk with non-AML compliant partners, explicit reference to compliance with all applicable AML, CTF and financial and economic sanctions legislations and regulations should be included in all partnership agreement between the Foundation and the partner.

Investments

It is not the core practice or decision of the Foundation to make or conduct any investment activities. However if the Foundation decided so and when the Foundation makes an investment, funds are made available to the recipients, thus the recipient (and its related parties such as beneficial owners and directors if the information is available) is subjected to sanctions screening. If the information of counterparties from any secondary market investment is available to the Foundation then such should also undergo sanctions screening. Re-screening of investments should be conducted regularly at least on an annual basis.

Know your employee ("**KYE**")

Sanctions screening, in addition to other applicable background checks should be conducted on all prospective employees and subsequent regular re-screening (at least on an annual basis) on all current employees should also be implemented.

New Digital Currencies, Products and Business Practices

The Foundation is required to identify and assess the money laundering / terrorist financing risks that may arise in relation to the development of new digital currencies, products, services and business practices, including new delivery mechanisms, and the use of new or developing technologies whether for new or existing solutions. In or der to do so, the Foundation will:

- undertake the risk assessment prior to the launch or adoption of such new digital currencies, products, services, business practices and technologies;

- take appropriate measures to manage and mitigate the risks; and

- document the risk assessment in writing.

4 RECOGNITION & REPORTING OF SUSPICIOUS TRANSASCTIONS AND SANCTIONS & WATCH-LIST SCREENING NAME MATCHES

Suspicious transaction recognition

All staff is responsible for reporting suspicious activities to the anti-money laundering unit of the Foundation or the Compliance Officer. All internal reported potentially suspicious activities must be reviewed by the anti-money laundering or compliance unit of the Foundation. All confirmed suspicious activities/transactions must be reviewed by the Compliance Officer, and the activities/transactions deemed non-suspicious after the anti-money laundering unit of the Foundation review should also be sample checked by the Compliance Officer regularly for quality assurance purpose. Staff should be reminded not to tip-off reported individuals (and other non-related parties) and keep the escalated cases confidential.

Suspicious transaction reporting

The Foundation must observe all legislations and regulations on suspicious transaction/activities reporting and have documented procedures to ensure the reporting procedure and timeline comply with local requirements. Any material cases must be reported to the Compliance Officer immediately via e-mail.

Whistleblowing

Staff who is aware of or has suspicion of any malpractice, compliance breach, illegal action or unethical activity in relation to AML / CTF / financial and economic sanctions should raise the concern with Compliance Officer immediately via e-mail to escalate the matter of concern.

Sanctions and watch-list screening name matches reporting

All potential matches / alerts from the screening system must be reviewed and investigated by the Foundation within 5 working days of notification, except for the ones generate from periodic full donors database re-screening or other unusual scenarios which is not part of usual operation and the alerts generated are not related to any new donors accepted. All alerts shall, regardless of the type of screening, be cleared as soon as possible to minimise sanctions risk. Any significant backlogs of alerts must be reported to the anti-money laundering or compliance unit of the Foundation with more detailed information and mitigation strategy.

Individual or entity matching to country sanctions lists

All potential country sanction matches (e.g. country prohibition alerts) with sufficient and accurate information on the donor must be escalated to the anti-money laundering or compliance unit of the Foundation via email for advice. Any confirmed true match to country sanctioned target must be escalated to the anti-money laundering or compliance

unit of the Foundation immediately. A report will be filed with the relevant local authorities with details of the donor and transaction.

5 COMMUNICATION, AWARENESS & TRAINING

Induction training on AML awareness to relevant new staff as well as refresher training to all relevant staff are mandatory. Induction training should be received by all relevant new staff within first four weeks of joining the business and refresher training should be received by all relevant staff at least annually.

Staff having no exposure to money laundering, terrorist financing or sanction risks can be exempted from the AML awareness training. Any exemption decision should be determined by the Compliance Officer with adequate record keeping on the decision.

All relevant staff should be made aware of and understand:

- The Foundation's AML policy;
- The legal obligations and regulatory requirements under which the Foundation operates;
- That they may be held personally liable if they fail to guard against money laundering and terrorist financing;
- Who serves as their Compliance Officer, how to contact him/her and the requirement to report any suspicions to him/her;
- The requirement to ensure that donors suspected of criminal activity are not alerted to those suspicious or the fact that they have been reported internally or to relevant authorities;
- The various offences that may constitute money laundering and terrorist financing;
- Legislations and regulations and other requirements measures and their legal and regulatory obligations and reporting requirements;
- Sanctions arrangements and that they should report suspected matches under the sanctions regime;
- The facilitation of tax evasion offence; and
- The penalty that may be incurred for failure to comply with AML, CTF and financial and economic sanctions requirements.

Employees should receive training appropriate to their roles to enable them to understand the money laundering and terrorist financing techniques which are likely to be used in their area of business. In particular, higher risk roles should be determined and additional role specific training should be designed and rolled out to these higher risk staff. This additional training should be delivered when these staff join the Foundation and be refreshed annually.

Post-training assessment with a minimum passing score must be implemented in both induction and refresher training to ensure the material is well understood. Case studies using examples from or relevant to the employees' jobs are useful to ensure that the training is appropriate. Training records must be tracked and documented. Completion rate should be monitored to aim for 100% attendance for all relevant staff. Appropriate follow up or disciplinary action should be considered for non-completion of mandatory training unless valid reasons can be obtained. The Foundation may prescribed specific centralised standards and tools for AML training to ensure consistency in the content and delivery of the training.

6 RECORD KEEPING AND INFORMATION SHARING

Records of information including but not limited to the following should be retained to ensure proper audit trail:

- Know Your Customer / Customer Due Diligence / Enhanced Due Diligence documents including application forms, copy of donor identification document, income proof documents, any internal analysis or recommendation, etc;
- Donation transaction records including payment information;
- Partners due diligence documents and related analysis or recommendation;
- Sanctions and watch-list screening record;
- Transaction monitoring and investigation decisions with supporting document on any additional research conducted and rationale of the decisions (for both confirmed suspicious transactions/activities and those deemed non suspicious);
- Reports to external authorities including suspicious transaction reports, sanctions matches and information submitted on court order or regulatory enquiry;
- Documents capturing significant correspondences and communication with external authorities such as regulator or law enforcement agency;
- Risk assessment with supporting documents and approval notes;
- Internal and external AML reporting documents;
- Compliance monitoring document including relevant plan, result and recommendation; and
- AML training records.

Records of information shall be retained for at least 7 years. The 7 years (or longer) timeframe should be counted from the completion of the event such as termination of customer relationship or suspicious cases reported to authorities.

The Foundation should establish and maintain procedures for data protection and sharing of information for the purposes of preventing money laundering and terrorist financing with other members of the Foundation.