



Anti-Money Laundering / Counter Financing Terrorism & KYC Policy – IFSCA (International Financial Services Centres Authority)

This document shall be treated as an appendix to Star Health's current AML Policy.

1. Introduction

1.1 Applicability

This Addendum is specific to **IFSCA (International Financial Services Centres Authority) guideline on AML/CFT/KYC, which is to be complied over and above existing AML CFT policy of SHAI by the Branch office, which is operating within GIFT City.**

This Addendum will be an integral part of the AML CFT policy of SHAI. This would be reviewed periodically based on the risk exposure and suitable changes (if any) be effected based on experience and to comply with the extant Act / Rules / Regulations and other applicable norms. In case of any modifications to be carried out after the review, the same will be approved by the Designated Director and subsequently, the same will be put up to the Board for approval.

2. Risk-Based Approach

SHAI adopts a Risk-Based Approach (RBA) to identify and assess the Money Laundering (ML) and Terrorist Financing (TF) risks to which it is exposed depending upon its nature of business and exposure to or involvement with certain types of clients, countries or geographic areas, products, services, transactions, or delivery channels, etc. and document the same. SHAI while adopting RBA shall ensure that,

- (i) The RBA is objective and proportionate to the risks;
- (ii) The RBA is based on reasonable grounds; and
- (iii) The RBA is reviewed and updated at appropriate intervals.

3. BUSINESS RISK ASSESSMENT

3.1 Identifying and Assessing business AML risks

A. SHAI shall:

- (a) take into consideration the nature, size and the complexity of its business activities and take suitable steps to identify its exposure to ML/TF risks;
- (b) consider the following risk factors, to the extent applicable and relevant, while identifying and assessing the ML/TF risks: -
 - (i) its type of customers and their activities;
 - (ii) its business engagement with the countries or geographic areas;
 - (iii) its products, services, delivery channels and activity profiles;
 - (iv) the complexity and volume of its transactions;
 - (v) the development of new products and new business practices, including new delivery mechanisms, channels and partners; and
 - (vi) the use of new or developing technologies for both new and pre-existing products;
- (c) based on the assessment and risk identification made at Clause (a) and (b) above, SHAI shall undertake commensurate mitigation measures.

3.2 New products, business practices and technologies

SHAI shall undertake the risk assessment exercise, prior to the launch or use of such products, practices and technologies and shall take appropriate measures to manage and mitigate the risks.

3.3. AML/CFT systems and controls

Anti-Money Laundering / Counter Financing Terrorism & KYC Policy – IFSCA

- (a) The nature and extent of AML/CFT systems and controls implemented by SHAI shall be commensurate with the ML/TF risks identified via the enterprise-wide ML/TF risk assessment, wherever applicable. SHAI shall put in place adequate policies, procedures, systems and controls to mitigate such ML/TF risks. The information obtained from the risk assessment shall be used to:
- (i) establish and maintain effective policies, procedures, systems and controls to prevent ML/TF;
 - (ii) Ensure that SHAI's AML/CFT Policies, Procedures, systems and controls adequately mitigate the risks identified under Clause 3.1 above;
 - (iii) Ensure SHAI's systems and control framework:-
 - (aa) includes a provision enabling its Senior Management to regularly review the information on operations and effectiveness of its AML systems and controls;
 - (ab) enable SHAI to determine:
 - (1) whether a customer or a Beneficial Owner is a Politically Exposed Person (PEP); and
 - (2) whether a beneficiary of the policy, or a Beneficial Owner of such beneficiary is a PEP, (in the cases where it is providing life insurance or other similar policies); and
 - (3) enable SHAI to comply with the Guidelines and applicable AML-CFT legislations.
 - (iv) ensure regular risk assessment is carried out on the adequacy of SHAI's AML/CFT systems and controls to enable it to identify, assess, monitor, manage and mitigate such risks adequately.

4. Assessing customer AML risks

(a) SHAI shall:

- (i) undertake a risk-based assessment of every customer; and
- (ii) assign the customer a risk rating proportionate to the ML/TF risks.

(b) The customer risk assessment referred to in Clause (a) above, shall be completed prior to undertaking Customer Due Diligence for new customers, and also where the SHAI otherwise feels necessary, for existing customers.

5. Wire Transfers

- 5.1.1. This Clause shall apply to a bank or SHAI when it sends funds by wire transfer or when it receives funds (including serial payments and cover payments) by wire transfer on the account of the wire transfer originator or the wire transfer beneficiary, but shall not apply to a transfer and settlement between the bank and another financial institution where the bank and the other financial institution are acting on their own behalf as the wire transfer originator and the wire transfer beneficiary, respectively.
- 5.1.2. SHAI shall monitor payment messages to and from high-risk countries or jurisdictions, as well as transactions with high risk countries or jurisdictions and suspend or reject payment messages or transactions with sanctioned parties or countries or jurisdictions.
- 5.1.3. Where name screening checks confirm that the wire transfer originator or wire transfer beneficiary is a terrorist or a terrorist entity, SHAI shall block, reject or freeze assets of these terrorists or terrorist entities immediately.

5.1.4. Where there are positive hits arising from name screening checks, they should be escalated to the Principal Officer. The decision to approve or reject the receipt or release of the wire transfer should be made at an appropriate level and be documented.

5.1.5. SHAI shall not omit, delete or alter information in payment messages, for the purpose of avoiding detection of that information during the payment process.

6. Record Keeping

6.1.1 SHAI shall preserve all necessary records, for at least six years or for such period as prescribed under the applicable laws, from the date on which business relationship has ended or transaction is completed.

6.1.2 SHAI shall provide to the Authority or any law enforcement agency immediately on request, a copy of a records maintained by it under these Guidelines.

6.1.3 Risk Assessment Documents

SHAI shall keep and maintain all risk assessment documents and provide to the Authority immediately on request, all relevant documents and information, including:

- (a) The business risk assessment undertaken;
- (b) How the business risk assessment was used for the purposes of undertaking a risk-based assessment of every customer; and assign the customer a risk rating proportionate to the ML/TF risks
- (c) the risk assessment of its customers undertaken and,
- (d) the determination of risk rating made