Anti-Money-Laundering & Counter-Terrorism Financing Policy

1. Introduction and Scope

The Singapore Shooting Association ("SSA") is registered as an Institution of a Public Character (IPC). As a registered charity under the Charities Act (Chapter 37), SSA is committed to observing the highest professional standards to safeguard its reputation and interests. Beyond adhering to best practices for commercial fund-raisers, SSA fully complies with Singapore's anti-money laundering and counter-terrorism financing regulations.

SSA maintains a zero-tolerance stance towards money laundering, terrorist financing, and all other forms of financial crime. We are fully committed to detecting, preventing, and mitigating the risks associated with such illicit activities.

This policy applies to all entities, Council Members, Secretariat staff, Ordinary Members, athletes, coaches, contractors, vendors, and third-party representatives operating with or on behalf of SSA. The SSA Board holds ultimate oversight of this AML Policy, while the Board Members and the General Manager (GM) are responsible for its day-to-day implementation.

2. Governance and Key Roles

The GM and the Finance Manager/Assistant Finance Manager shall jointly assume the role of the Money Laundering Reporting Officer (MLRO). The MLRO is responsible for the implementation, monitoring, and enforcement of SSA's AML compliance program.

3. Internal AML Policy and Risk-Based Approach

SSA's Internal AML Policy establishes procedures for compliance and monitoring using a risk-based approach. While SSA does not typically receive large donations from the public or transact with unidentified entities (aside from appointed contractors and vendors), we recognize the importance of identifying and managing overall money laundering risks.

A critical component of our strategy is a robust Customer Due Diligence (CDD) process. Staff must ensure they deal only with legitimate customers by verifying their identities, assessing their risk levels, and conducting ongoing monitoring.

Understanding the common indicators of suspicious activity (refer to **Annex A** – Red Flag indicators) is essential for real-world detection and prevention.

- Key Customer Due Diligence (CDD) and Know Your Customer (KYC) procedures include:
- Identity Verification: Verifying the identities of customers, partners (where applicable), and beneficial owners before establishing or continuing a business relationship.
- Originator Verification: Identifying the originator of any value transfer and taking the necessary measures to verify their identity.
- Transaction Recording: Recording all relevant details of a value transfer, including (but not limited to) the date, type and value of the asset transferred, and the value date.
- Record Keeping: Maintaining all customer identification documents and transaction records for a minimum of five (5) years, in compliance with local regulations.
- Ongoing Monitoring: Conducting regular assessments to identify and evaluate specific money laundering risks. This involves actively monitoring for unusual transaction patterns or suspicious activities, with particular attention to:
- Telegraphic or electronic transfers of funds on behalf of a person to another person.
- Transmission of funds between Singapore and a foreign country, or between foreign countries, on behalf of a person.
- Abrupt surges in account activity, large and frequent deposits, or transactions inconsistent with a customer's known financial history.
- Discrepancies between the scale of financial activity and the customer's known profession, lifestyle, or business model (e.g., a student making large, unexplained transfers).

4. Reporting Suspicious Activities

Clear escalation paths with well-documented processes are vital. All staff and Board members are required to report any suspected money laundering activity immediately to the MLRO.

The MLRO will evaluate the report and, if necessary, file a confidential Suspicious Activity Report (SAR) with the relevant financial authorities to ensure timely regulatory compliance. Internal reviews and reporting must be conducted without delay.

5. Training and Record Keeping

SSA is committed to providing regular staff training programs to enhance employee awareness and vigilance. These programs equip staff with the knowledge to identify and report potential money laundering risks effectively, in collaboration with relevant government authorities.

SSA will maintain training records for all staff who have completed mandatory, regular training on AML regulations, red flag indicators, and internal reporting procedures.

6. Non-Compliance

Violations of this policy may result in disciplinary action, up to and including termination of employment or engagement. Individuals found to be in violation may also be subject to civil or criminal penalties under Singapore law.

Prepared by: Lim Tian Lye (GM)

Approved by: SSA Council

Date of Issue: 11 July 2026