Anti-Money Laundering Policy

THIS POLICY APPLIES TO:

- MST Golf Group Berhad (Registration No.: 199301009307 (264044-M))
- MST Golf Sdn Bhd (Registration No.: 198901011987 (189294-P))
- MST Golf Management Sdn Bhd (Registration No.: 200101013452 (549209-A))
- MST Golf Arena Sdn Bhd (Registration No.: 199801015399 (471528-D)
- MST Golf (Singapore) Pte Ltd (Registration No.: 200002124N)
- PT MST Golf Distribution (AHU-0068036.AH.01.01.TAHUN 2023)
- PT MST Golf Indonesia (AHU-0067107.AH.01.01.TAHUN 2023)
- Unless otherwise specified, any other companies that may become subsidiaries of MST Golf Group Berhad after the effective date of this document.

ADOPTION & REVISION HISTORY:

Rev.	Effective Date	Description	Approved by
0	1 Oct 2024	Formal Adoption	Board of Directors

(SEE NEXT PAGE FOR POLICY)

1. INTRODUCTION

1.1. MST Golf Group Berhad ("Company") and its subsidiaries listed on the cover page of this document (collectively including the Company, "Group") are dedicated to conducting their businesses in a lawful and ethical manner, ensuring compliance with all latest and applicable anti-money laundering ("AML") laws and regulations in the countries where it operates, including but not limited to:

1.1.1. Anti-Money Laundering, Anti-Terrorism Financing, and Proceeds of Unlawful Activities Act 2001 ("AMLA") in Malaysia;

1.1.2. Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 ("CDSA") in Singapore; and

1.1.3. Equivalent or similar laws in Indonesia and other countries where the Group operates.

1.1. The Group adopts this Anti-Money Laundering Policy ("Policy") to prevent, detect, and report any money laundering activities within the Group's operations.

2. OBJECTIVES AND SCOPE

2.1. The purpose of this Policy is to outline the Group's commitment to preventing money laundering and to establish clear guidelines and procedures for identifying, managing, and reporting suspicious activities. The Policy also ensures compliance with relevant AML laws and regulations.

2.2. This Policy applies to all aspects of the Group's business operations, including customer interactions, transactions, and relationships with third-party vendors, suppliers, and partners.

2.3. All employees, officers, directors, contractors, consultants, and third parties acting on behalf of the Group are required to adhere to the procedures outlined in this Policy.

3. KEY DEFINITIONS

3.1. **Money Laundering:** The process of concealing the origins of illegally obtained money, typically by means of transfers involving foreign banks or legitimate businesses.

3.2. **Customer Due Diligence ("CDD"):** A process used to verify the identity of customers and assess their potential risk for money laundering or terrorist financing.

3.3. **Enhanced Due Diligence ("EDD"):** A more rigorous form of Customer Due Diligence required for high-risk customers or transactions. EDD involves additional measures to verify the customer's identity and assess the purpose and intended nature of the business relationship.

3.4. **Beneficial Owner:** The individual or entity that ultimately owns or controls a customer or the rights to a particular asset.

3.5. **Suspicious Activity Report ("SAR"):** A report filed with the relevant authorities when suspicious activity is detected that could be related to money laundering or terrorist financing.

4. HIGH-RISK CUSTOMERS

4.1. High-risk customers are individuals or entities that present a higher potential for being involved in money laundering, terrorist financing, or other illegal activities. These customers require Enhanced Due Diligence (EDD) and closer monitoring due to their risk profile. High-risk customers typically include:

4.1.1. **Politically Exposed Persons (PEPs):** Individuals who hold or have held prominent public positions, such as heads of state, government ministers, military leaders, or senior executives of state-owned enterprises. Due to their position and influence, PEPs may be more susceptible to corruption and bribery.

4.1.2. **Customers from High-Risk Jurisdictions:** Customers based in or conducting transactions in countries with weak AML regulations, significant levels of corruption, or areas known for financing terrorism. These jurisdictions are often identified by international bodies like the Financial Action Task Force (FATF).

4.1.3. **Customers Engaged in Cash-Intensive Businesses:** Businesses that deal predominantly in cash, such as casinos, money service businesses, and currency exchanges, are considered high risk because cash transactions are harder to trace and verify.

4.1.4. **Non-Profit Organizations and Charities:** Although most operate legitimately, some non-profits can be misused to funnel funds for illegal activities, including terrorism financing.

4.1.5. **Customers with Complex Ownership Structures:** Companies with complicated or opaque ownership structures, especially those involving offshore entities or trusts, may be used to hide the true beneficial owners and the source of funds.

4.1.6. **Customers Involved in High-Value or High-Volume Transactions:** Individuals or entities that frequently engage in large or irregular transactions, particularly

those that are inconsistent with the customer's known business or personal profile.

4.1.7. **Customers with No Face-to-Face Interaction:** Remote or non-face-to-face transactions, such as those conducted online, pose a higher risk because it's harder to verify the identity of the customer.

4.1.8. **Customers with Unusual Transaction Patterns:** Customers whose transactions deviate significantly from their typical behavior or the expected patterns for their industry or profile.

4.1.9. **Customers Using Private Banking or Wealth Management Services:** These services often cater to high-net-worth individuals and may involve complex financial products and transactions, which can increase the risk of money laundering.

4.1.10. **Newly Established Businesses with No Financial History:** Startups or businesses with limited or no financial track record may pose a higher risk, particularly if the source of their initial funding is unclear.

5. ROLES AND RESPONSIBILITIES

5.1. Employees

5.1.1. Employees are required to understand and comply with the Policy.

5.1.2. Employees must perform Customer Due Diligence (CDD) when establishing business relationships, especially with high-risk customers or those from high-risk jurisdictions.

5.1.3. Employees are responsible for identifying and reporting suspicious activities to the Finance Department.

5.2. Finance Department ("Finance Dept")

5.2.1. The Finance Dept is responsible for overseeing the implementation of the Policy and ensuring compliance with applicable laws and regulations.

5.2.2. The Finance Dept is responsible for filing Suspicious Activity Reports (SARs) with the appropriate authorities when necessary.

6. CUSTOMER DUE DILIGENCE (KNOWING YOUR CUSTOMERS, "KYC")

6.1. **Identification and Verification:** The Group requires thorough identification and verification of customers before establishing any business relationship. This process includes:

6.1.1. **Obtaining Customer Information:**

Individuals:	**Entities:**
(a) Full legal name. (b) Date of birth. (c) Residential address. (d) Nationality. (e) Identification number (e.g., NRIC, passport number). (f) Contact details (phone number, email address).	(a) Full legal name. (b) Registration or incorporation number. (c) Date of incorporation. (d) Registered office address. (e) Principal business activities. (f) Names of directors, partners, or trustees. (g) Identification of the beneficial owner(s).

6.1.2. **Verification of Identity:**

Individuals:	**Entities:**
(a) Verify the identity of individuals using valid, government-issued photo identification (e.g., national identity card, passport, driver's license). (b) Cross-check the identification details with independent and reliable sources, such as government databases or credit bureaus.	(a) Verify the legal status of the entity by obtaining and reviewing certified copies of the certificate of incorporation or registration. (b) Obtain and verify the entity's constitution or other governing documents (e.g., memorandum and articles of association). (c) Confirm the identity of directors, partners, or trustees through government-issued identification documents. (d) Identify and verify the beneficial owners using official documents, such as a shareholders' register, or declarations from the entity.

6.1.3. **Understanding the Nature of the Business Relationship:** Determine the purpose and intended nature of the business relationship, including:

(a) The type and frequency of transactions expected.

(b) The source of funds to be used in the relationship.

(c) The source of wealth (for individuals) or funding (for entities).

(d) The anticipated account activity, including the types of transactions, volume, and frequency.

6.2. **Enhanced Due Diligence (EDD):** For High-Risk Customers, the Group will implement EDD, which involves additional scrutiny and verification measures:

6.2.1. **Additional Verification Steps:**

(a) Obtain senior management approval before establishing or continuing a business relationship with High-Risk Customers.

(b) Perform more in-depth verification of the customer's identity and source of funds/wealth, such as:

i. Reviewing additional identification documents.

ii. Conducting background checks or seeking references from other financial institutions.

iii. Verifying the legitimacy of the customer's source of wealth or funding by reviewing financial statements, tax returns, or other relevant documents.

(c) Implement ongoing monitoring with more frequent reviews of the customer's transactions and account activities to identify any suspicious behavior.

6.2.2. **Ongoing Monitoring and Periodic Review:**

(a) High-Risk Customers will be subject to continuous monitoring to ensure that their activities remain consistent with their known profile and expected behavior.

(b) Periodically review and update customer information, particularly for high-risk customers, to ensure that records are current and accurate.

(c) For PEPs and customers with complex structures, conduct a thorough review of the relationship at least annually, including a reassessment of the customer's risk profile.

7. REPORTING AND RECORD-KEEPING

7.1. Suspicious Activity Reporting

7.1.1. Employees must report any suspicious activity to the Finance Dept without delay. The Finance Dept will evaluate the report and, if deemed necessary, file a Suspicious Activity Report (SAR) with the relevant authorities.

7.2. Record-Keeping

7.2.1. The Group is required to maintain records of all customer due diligence, transactions, and suspicious activity reports for a minimum period as required by law. These records must be securely stored and readily accessible for review by relevant authorities.

7.3. Confidentiality

7.3.1. Employees must safeguard all customer information with strict confidentiality measures, in compliance with applicable data protection laws as well as the Group's Personal Data Protection Policy and other policies and code of conduct relevant to confidentiality.

8. SANCTIONS AND PROHIBITED ACTIVITIES

8.1. The Company or any of its subsidiaries will not engage in any business with individuals, entities, or countries that are subject to international sanctions mandated by the government of the country in which it operates. Employees must screen customers and transactions against relevant sanctions lists and report any matches to the Finance Dept.

9. TRAINING AND AWARENESS

9.1. The Group is committed to providing regular AML training to all employees to ensure they understand their responsibilities under this Policy. Training will include updates on legal requirements, red flags for money laundering, and procedures for reporting suspicious activities.

10. COMPLIANCE AND DISCIPLINARY MEASURES

10.1. Non-compliance with this Policy or relevant AML laws may result in disciplinary action, including termination of employment. The Group also reserves the right to terminate relationships with third parties who fail to comply with this Policy.

11. REVIEW AND UPDATES

11.1. This Policy will be reviewed and updated regularly to ensure it remains compliant with any changes in AML laws and regulations in the countries in which the Group operates.

-END-