ANTI-MONEY LAUNDERING POLICY

September 2024

HD HYUNDAI MARINE SOLUTION

Anti-Money Laundering and Counter-Terrorist Financing Policy

1. Introduction

This Anti-Money Laundering and Counter-Terrorist Financing Policy (the "AML Policy") defines responsibilities and policies for HD Hyundai Marine Solution Co Ltd and all of its subsidiaries and affiliates (collectively, the "Company") with regard to avoiding money laundering and terrorist financing activities. Company is committed to conducting its business in accordance with the highest legal and ethical standards, and in a manner consistent with all applicable U.S. and non-U.S. laws, rules and regulations. The Company has adopted this AML Policy to prevent Company from being used to launder money or finance terrorism, and to comply with applicable anti-money laundering ("AML") and counter-terrorist financing ("CTF") laws. This AML Policy applies to all directors, officers, and employees of the Company, regardless of location or nationality (collectively, "Company Personnel") and should be read in conjunction with Anti-Corruption policy and Sanctions policy as well as any applicable policies and procedures.

What is money laundering?

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have been derived from legitimate origins or constitute legitimate assets. The process of money laundering is used to conceal the true origin of funds gained through activities such as fraud, corruption, tax evasion, and drugs trafficking. If undertaken successfully, the process facilitates the appearance of legitimacy for such funds.

This AML Policy is intended to provide Company Personnel of the Company with high-level guidance on identifying potential money laundering activity and understanding the procedures that the Company requires all Company Personnel to follow in order to prevent the Company becoming involved with such activity.

Money laundering can take many different forms, in some cases the transfers involved can be relatively simple whilst in other situations there may be a complex web of transactions. Generally, there are three main stages of laundering money – placement, layering and integration.

Placement: Funds derived from illegal activities are deposited into the financial system. A way needs to be found of introducing funds into the financial system.

Layering: Confusing the trail in order to disguise the source and ownership of funds. Once the funds are in the system it is necessary to obscure the original entry point by entering into numerous transactions and movements making the funds harder to trace.

Integration: Funds are returned to the original source but appear to originate from a legitimate source. A final transaction takes place which returns the funds to the beneficial ownership of the individual/entity that initiated the process. However, the funds now appear to have been acquired through legitimate activity/transactions.

What is terrorist financing?

Terrorist financing occurs when people gather funds to support terrorists, terrorist activities, or terrorist groups. In contrast to money laundering, terrorist financing can involve the use of legally derived money to carry out illegal activities.

Know Your Customer and Customer Due Diligence

The Company's know-your-client ("KYC") and customer due diligence procedures (please refer to sections 6 and 7 for more detail) are integral parts of the Company's compliance system. These procedures assist the Company to identify and verify each counterparty to ensure the Company does not become involved with a business or individual with a history of financial crime, or sanctions.

The KYC process involves the verification of the customer's identity by gathering relevant evidence and information about the transaction parties. Whereas the customer due diligence is a process which continues after the customer has been onboarded, and includes checks like sanctions and Politically Exposed Person screenings, to continuously assess the risk-level of a customer.

Applicable laws

As a global organization, the Company applies internationally recognized, industry standards to its AML procedures as recommended by organizations such as The Financial Action Task Force. Failure to comply with the relevant legal standards can result in criminal sanctions for both individuals and entities including fines and/or imprisonment.

Company Personnel have an affirmative obligation under applicable AML/CTF laws in some jurisdictions where the Company conducts business to promptly escalate and report all relevant facts concerning situations where there is evidence or suspicion of money laundering. It is an offence to assist in the process of money laundering, including tipping off a money launderer regarding an investigation or failing to report knowledge/suspicions that money laundering is taking place.

2. Scope

This AML Policy applies to Company Personnel. In addition, this AML Policy also applies to the Company's subsidiaries, affiliates and all third parties acting on behalf of the Company, such as agents, resellers, distributors, joint venture partners, suppliers, vendors and other representatives ("Third-Party Intermediaries").

3. Non-compliance with this AML Policy

Preventing money launderers from using Company is of paramount importance and requires the cooperation of Company's employees and any other personnel authorized to act on behalf of the Company. Any involvement in money laundering activity–even if inadvertent–could result in potential civil and criminal penalties for the Company and its employees, as well as possible forfeiture of assets. Association with money laundering also could cause significant

and long-term harm to Company's reputation. Accordingly, Company will take all reasonable and necessary steps to prevent itself from being used to launder funds derived from illegal activities. Non-compliance with this AML Policy may subject an employee of other personnel authorized to act on behalf of the Company to disciplinary action, including termination of employment.

4. Responding to Incidents of Noncompliance

If Company Personnel are aware of an actual or potential violation of this AML Policy, alert Legal Affairs Team(Compliance). Do not disclose (or "tip off") to the counterparty, your colleagues or anyone else outside of the Company the fact that Company Personnel have reported an actual or potential match to individuals, entities or restricted countries with whom the Company is prohibited to deal with under applicable AML/CTF laws.

Non-compliance with this AML Policy may subject involved Company Personnel to disciplinary action, depending on the severity of the violation, up to and including termination of employment, as well as possible civil or criminal fines or penalties.

5. AML Policy Statement

Company Personnel may not facilitate, participate, or provide assistance in any money laundering activity or terrorist financing activity regardless of where the activity takes place. Since the Company is operating or doing business in multiple jurisdictions, it must comply with applicable AML/CTF laws in those jurisdictions.

Company Personnel have a duty to report violations, or suspected violations, of the AML Policy to the Legal Affairs Team(Compliance). Non-compliance with the AML Policy will subject any involved Company Personnel to disciplinary action, which may include fines, termination of employment, and/or possible civil or criminal penalties.

Any Company Personnel with questions regarding the AML Policy should contact Legal Affairs Team(Compliance).

6. Customer Due Diligence

The Company must be confident in the integrity of parties with whom it deals. Such confidence is obtained by gathering relevant information about transaction parties and performing risk-based due diligence to confirm that such parties are not individuals, entities or restricted countries with whom the Company is prohibited to deal with under applicable AML/CTF Laws in South Korea or elsewhere.

Risk-based due diligence on counterparties should include the following steps:

- Identify and verify the prospective counterparty.
- Obtain information on the purpose and intended nature of the business relationship with the counterparty.
- Identify the country of origin or operation.

The Company must exercise ongoing due diligence, as appropriate, with respect to its ongoing relationships with the counterparty, including monitoring transactions in order to ensure that the transactions are consistent with the Company's knowledge of the counterparty, and the counterparty's business and risk profile, and the nature of transactions to be conducted with the Company, taking into account, where appropriate, the counterparty's source of funds.

7. Monitoring Suspicious Activity

Company Personnel are responsible for monitoring potentially suspicious activities or "red flags" related to transactions, counterparties, customers, or Third-Party Intermediaries (for further details on suspicious activities/"red flags" please refer to *"*Payment irregularities*"* section below). If any Company Personnel identifies suspicious activity in connection with a proposed transaction, he/she is required to notify Legal Affairs Team(Compliance) before the transaction is processed.

The Company may be required to file suspicious activity reports with relevant authorities in some jurisdictions when, in the course of business, Company Personnel may come to know, suspect, or have reasonable grounds to know or suspect that a transaction or a pattern of transactions involves funds derived from illegal activity or otherwise triggers AML/CTF reporting requirements. **It is critical that Company Personnel raise concerns to Legal Affairs Team(Compliance) as described in this section so that the Company can comply with its obligations.**

There are two key issues that may indicate higher money laundering risk of which all Company Personnel should be aware, counterparties integrity concerns and payment irregularities.

Counterparty Integrity

KYC procedures form the foundation of its AML controls and are designed to identify any potential counterparty integrity issues at the very start of any new relationship.

The level of due diligence undertaken on a counterparty depends on a number of risk factors based upon applicable AML guidance. These risk factors include type/structure of a company or a Third-Party Intermediary, country of incorporation, location of bank account, political connections/exposure, volumes of transactions, and nature of business activity.

The Company's KYC procedures include ongoing monitoring and periodic due diligence reviews for counterparties even after they have been initially approved. This is to ensure new risks that develop during the life cycle of a relationship are appropriately taken into account.

All Company Personnel must report any concerns that they may develop regarding a counterparty to Legal Affairs Team(Compliance).

Payment irregularities

It is also important to consider any increased money laundering risks which may occur on specific transactions. There is a variety of indicators / "red flags" that Company Personnel should be aware of.

The following are illustrative examples of a counterparty or a Third-Party Intermediary conduct that should be brought to the immediate attention of Legal Affairs Team(Compliance).

- Payments made in currencies other than that specified in the invoice.
- Attempts to make payments in cash or cash equivalents.
- Payments made by someone not a party to the contract.
- Payments to/from an account other than the counterparty's normal business relationship account.
- Requests or attempts to make payments for an invoice or a group of invoices by multiple cheques or transfers.
- Requests to make an overpayment.
- Refusal to provide standard identifying information.
- Unusual concerns are raised regarding the Company's compliance with AML laws.
- Refusal to reveal any information about business activities.
- Provision of unusual or suspect identification or business documents.
- News reports indicating criminal, civil or regulatory violations.
- Difficulty in describing the nature of its business or lack of general industry knowledge.
- When acting as agent or nominee for another individual or entity, refusal (without legitimate commercial reasons) to provide any information in response to questions about the other entity

8. Recordkeeping

The Company must keep full and accurate records of the transaction and data obtained for due diligence, identification and verification process, as well as the Company's monitoring and compliance with this AML Policy.

The Company may be required to furnish regulators with information contained in records under relevant AML/CTF laws. Any request by regulators for such records must be referred to the Legal Affairs Team(Compliance).

9. Monitoring and Reporting

The Legal Affairs Team(Compliance) is responsible for the administration of this AML Policy, including implementing documented procedures to enable compliance, monitoring and reporting, as well as coordinating training as required.

10. Certification

As part of the Company's ongoing commitment to AML/CTF compliance, all Company Personnel must receive and review a copy of this AML Policy.

Company Personnel must then certify in writing that they (1) have reviewed the AML Policy, (2) agree to abide by the AML Policy, and (3) agree to report any potential violations of the AML Policy.

Addendum

This AML Policy shall be effective from November 26, 2021.

Addendum

This AML Policy shall be effective from September 25, 2024.