

LOKESH MACHINES LIMITED

**EXPORT CONROLS AND
ECONOMIC SANCTIONS**

COMPLIANCE POLICY

JANUARY 2025

LOKESH MACHINES LIMITED

EXPORT CONTROLS AND ECONOMIC SANCTIONS COMPLIANCE POLICY

January 2025

Executive Summary

Lokesh Machines Limited (hereinafter referred to as “**LML**” or the “**Company**”) is committed to complying with all applicable trade regulations, including economic sanctions and export controls. Although we are an Indian company, we have non-Indian customers, vendors, and business partners around the globe, and we also conduct transactions in foreign currencies. We must be alert to how trade regulations affect our international business. This Export Control and Economic Sanctions Compliance Policy (the “**Policy**”) sets forth the Company’s procedures for complying with the laws wherever the Company does business.

It is the policy of the Company to comply with applicable export control and sanctions laws. LML expects all Company directors, officers, employees, contractors, and other persons working under the Company’s managerial supervision, including all individuals employed by any entity, owned and/or controlled by the Company (the “**LML Team**” or “**Company Team**”) to comply with this Policy, as well as customers, vendors, agents, or any natural or legal persons who have agreed to become a buyer/supplier of the Company’s products or services. All such persons have an important role to play in safeguarding LML’s reputation, legal and financial interests, and upholding its policies. The LML Team plays a key role in helping the Company comply with applicable regulations.

The objective of this Policy is to inform the Company Team of the key principles of trade sanctions laws where the Company or any of its subsidiaries may require and to set out regulations on how to fulfil these legal requirements in accordance with established best practices. This includes the screening of obligations under trade sanctions laws as well as a description of the internal organisation and processes in relation to trade sanctions, and of the consequences in case of non-compliance with this Policy.

For the avoidance of any doubts, it is stated here, where stricter requirements apply in countries in which the Company operates, any such requirements must be observed irrespective of, and in addition to, this Policy. The Policy applies to businesses of the Company including employees, affiliates, and any other persons authorised to represent or act on behalf of the Company.

The Company Team plays a key role in helping the Company comply with applicable sanctions regulations. It is your responsibility to read and understand this Policy. Trade laws are dynamic in nature and may change. This Policy serves as guidance and must not be read to cover any/all global sanctions/ eventuality, and therefore, it is your responsibility to seek additional guidance from the Company’s legal department (the “**Legal Department**”) whenever you have any question or doubts as to how these rules apply to a particular transaction or situation. In certain cases, based on the relevant factors and risk assessment evaluation, the Board of Directors of the Company (the “**Company’s Board**”) may allow exclusions from application of this Policy, subject to applicable laws and a legal risk assessment.

This Policy has been divided into Part A, which outlines the general principles and guidelines on sanctions, Part B which sets out the procedural aspects for undertaking recommended sanctions compliant measures and Part C, which has the appendices including additional information on export control and sanctions laws, potential red flags and sample sanctions clause and know your customer forms.

The contact information for the Legal Department is as follows:

Name: Gurprit Singh

Designation: Company Secretary & Compliance Officer

Address: B29, EEIE, Stage II, Balanagar, Hyderabad- 500037 Telangana, India

Contact Information: Email Id: cosecy@lokeshmachines.com, Mb: +91 70322 28196

Signature: _____

Name: Mullapudi Srinivas

Designation: Whole-time Director

CONTENTS

PART A: GENERAL GUIDELINES	4
1. INTRODUCTION	4
2. EXPORT CONTROLS.....	5
3. ECONOMIC SANCTIONS.....	6
4. TRANSACTIONS SUBJECT TO COMPLIANCE REVIEW	8
5. RECUSAL POLICY	8
PART B: PROCEDURAL MANUAL	11
1. GUIDELINES FOR THE COMPANY TEAM	11
2. RISK ASSESSMENT.....	11
3. ROLE OF THE LEGAL DEPARTMENT.....	13
4. QUARTERLY COMPLIANCE REPORTS	14
5. IMPLEMENTATION OF THE COMPLIANCE POLICY	14
6. RECORD RETENTION	14
7. TRAINING OF EMPLOYEES.....	15
8. QUESTIONS AND ESCALATIONS.....	15
9. VIOLATIONS OF POLICY AND PROCEDURE	16
PART C: APPENDICES	17
APPENDIX-1A: EXPORT CONTROL LAWS	17
OVERVIEW OF INDIAN EXPORT CONTROLS	17
OVERVIEW OF U.S. EXPORT CONTROLS.....	17
OVERVIEW OF UK/EU EXPORT CONTROLS	18
APPENDIX 1B: SANCTIONS LAWS	19
OVERVIEW OF INDIAN SANCTIONS LAWS	19
OVERVIEW OF U.S. SANCTIONS.....	19
OVERVIEW OF EU AND UK SANCTIONS.....	21
APPENDIX 2	22
EXHIBIT A: COUNTER-PARTY KYC INFORMATION	22
EXHIBIT B: LML’S STANDARD OPERATING PROCEDURE (SOP) FOR IMPLEMENTING THE POLICY	25
EXHIBIT C: RED FLAGS	27
EXHIBIT D: SANCTIONS COMPLIANCE CLAUSES FOR AGREEMENTS/CONTRACTS	29

PART A: GENERAL GUIDELINES

1. INTRODUCTION

1.1 Overview of the types of trade regulations covered in the Policy

Countries impose export controls and economic sanctions measures against foreign countries, entities, and individuals to achieve a variety of foreign policy and security objectives, or as a result of the decisions of international bodies such as the United Nations Security Council.

Export Controls. Export controls limit the transfer of goods and technologies between countries or, in some cases, between different parties within a single country, or between persons of different nationalities within a country. The relevant export controls may include not only the country that the items are in, but also the country where the items originated.

Economic Sanctions. The United Nations, India, the United States, the Member States of the European Union, and other countries have adopted economic sanctions laws that restrict activities and transactions with, in or involving certain specified sanctioned countries, their nationals, and other designated entities (including vessels) and individuals. The restrictions on the sale and/or shipment of products, as well as related activities, often apply regardless of the location from which the sale or shipment originates.

Please note that some jurisdictions' economic sanctions have extraterritorial effect, even when all parties are located outside the jurisdiction or when only local currencies are used. For example, some U.S. sanctions apply to non-U.S. individuals and entities (these are known as “**secondary sanctions**”).

Broadly, the Economic Sanctions Laws which are most likely to impact the LML Team can be categorised into:

- a) Restrictions on dealings with certain individuals or companies (“**Sanctioned Persons**”)
- b) Restrictions on certain types of trade with certain countries (sanctioned activities)

1.2 Consequences of violating international trade laws

Breaches of international trade laws may result in serious legal and reputational consequences for the Company including civil and criminal fines and loss of export or import privileges, and it could also expose the Company and the Company Team members to civil and criminal consequences which may include penalties and/or imprisonment. The consequences of non-compliance are determined in accordance with the applicable national law, and thus, may vary from jurisdiction to jurisdiction.

Non-compliance also poses a substantial reputational risk for the Company and could impact the Company’s relationships with counterparties, harming its ability to conduct business, especially in countries with extremely high ethical and security standards.

2. EXPORT CONTROLS

2.1 General summary of export control principles

It is important to be aware of, and understand the relevant applicable export controls when transferring goods across international borders, to nationals of a different country. Export controls may apply to exports as well as re-exports. In respect of these, it is recommended to:

- a. identify any export-controlled items with which you deal, including the countries that control them;
- b. be aware of the existing restrictions on controlled items, including required authorisations and licenses;
- c. comply with relevant export controls whenever exporting, re-exporting, or transferring within a country, controlled items; and
- d. check with the Legal Department whenever you are unsure whether an item is subject to export controls, whether the transfer of a controlled item complies with export controls, or whether the transfer of a controlled item requires prior authorization from the relevant government(s).

2.2 Basic rules for export controls

The Company Team must observe the following basic rules to ensure compliance with export controls:

a. **Be aware of controlled items**

Not every item is subject to export controls. Many major economies, including India, use a common list of “dual-use” controlled goods and technologies. If you are involved in sending goods or technologies out of India, you should understand which items are typically controlled and be aware of the need to examine whether licensure is required.

Be aware that if an item is of U.S. origin, contains U.S. origin materials or components, or is the direct product of U.S. technology, the item may be subject to U.S. export controls even if it is not specifically identified on the U.S. export control list.

If you are unsure whether an item you wish to export or transfer is controlled or such export or transfer is permissible, you must consult with the Legal Department before proceeding. It is possible that you may require an authorisation or license to export, re-export, or otherwise transfer controlled items.

b. **Identify which country’s export controls apply**

Typically, applicable export control regimes will include both the country where the items or technology to be exported are located, and the original country of origin; many goods that are controlled upon the original export remain controlled upon re-export from a third country.

If you are unsure about which country's export controls, if any, apply to an item, you must consult with the Legal Department before exporting or re-exporting the item.

c. **Comply with relevant export controls whenever exporting or re-exporting controlled items.**

You should be familiar with controls applicable to transactions typical for your function, and you should consult the Legal Department in unfamiliar transactions. On a risk basis, you must do sufficient diligence to understand the ultimate enduser and enduse of any item or technology proposed to be exported; prohibited transactions conducted through intermediaries are still prohibited.

For example, goods may be sold from India to Country A, for onward delivery to Country B, and the export control laws of both countries may be implicated. Goods sold or manufactured in one country may be resold from the inventory to a different country and may be subject to the laws of both countries.

d. Export controls may result in the export or transfer of a product being prohibited altogether, or the transfer may be restricted as to certain destinations, end users or end uses. Export controls may also require that exporters obtain export licenses from relevant export authorities prior to any transaction. If it appears that goods may be subject to export licensing requirements the Legal Department can provide assistance with proper completion of any licensing forms or applications. **Be aware of diversion risks.**

You should be alert of the possibility that a prospective purchaser of a product located in one country, to which the export can be made lawfully, may be acting on behalf of the actual intended end user in another country, to which an export authorization would be required.

If you become aware of, or have reason to believe, that the prospective buyer is not going to be the actual end user of the product, you must consult with the Legal Department before exporting or re-exporting the item.

Please refer to Appendix IA for jurisdiction-wise export controls.

3. ECONOMIC SANCTIONS

3.1 General summary of economic sanctions

LML and its directors, officers and employees shall fully comply with all applicable sanctions laws, in particular those of India, the United States, the European Union, the United Kingdom, the United Nations, and other relevant countries.

Due to the imposition of sweeping sectoral sanctions that are directly related to LML's business activities, **the Company will not engage, directly or indirectly, in any business with or connected to Russia, Belarus, or any country subject to sectoral sanctions** without the approval of the Company's Board.

Due to the imposition of comprehensive economic sanctions and embargoes against certain countries, **the Company will not engage, directly or indirectly, in any business with or connected to Cuba, Iran, Syria, North Korea, Venezuela, and the Crimea, Donetsk, and Luhansk Regions of Ukraine.**

The Company and the Company Team members must pay careful attention to all relevant sanctions laws. The Company Team must monitor the Company's transactions to ensure compliance with applicable economic sanctions. In many instances, a single transaction will be subject to the laws of more than one country. Moreover, transactions using another country's currency, may become subject to that country's economic sanctions rules.

The Company's senior management is committed to fostering a culture of compliance. To ensure compliance, this commitment must be upheld by all members of the Company Team. This section describes your responsibilities with regard to compliance with applicable sanctions laws and provides an overview of sanctions laws, primarily in India, the U.S., UK, and the EU.

3.2 Basic rules for economic sanctions

The Company Team must observe the following basic rules to ensure compliance with economic sanctions:

a. **Be aware of sanctions targets**

Sanctions laws are constantly changing. Be aware of countries and companies that may be the target of one or more sanctions regimes. If you encounter a transaction or business relationship that has any relationship to a sanctioned or otherwise high-risk country, company, or individual, you must consult with the Legal Department to ensure LML's business activities comply with all relevant laws and regulations. If a counterparty raises sanctions concerns, always escalate them to the Legal Department.

b. **Undertake Know Your Customer ("KYC") diligence**

LML is responsible for conducting risk-based due diligence to verify the true identity and ownership of parties to a transaction and whether parties to a transaction are acting for a sanctioned party or individual. If you become aware or suspect that any party to a transaction has any direct or indirect connection to a sanctioned person or country, consult the Legal Department.

Please refer to Part-B Section 2 for risk assessment.

Please refer to Appendix 2 Exhibit A for sample KYC Form.

c. **Obtain contractual assurances**

All transaction documents, including but not limited to commercial invoices and sales agreements, must include an assurance stipulated under a sanctions compliance clause that the goods being sold are not intended for direct or indirect export to a sanctioned country, entity, or individual.

Please refer to Appendix 2 Exhibit D for sample sanctions clause.

d. **Operate with transparency**

Do not conceal the real identity of any party to a transaction in order to evade sanctions or banking difficulties, and if any other party requests that you do so or asks you to create or alter documents in a misleading manner or to obscure the

enduser or shipment destination, you must notify the Legal Department immediately.

e. **Be diligent about structures of transactions**

You know what transactions are normal in your market. If you know or suspect that a transaction is being structured to hide something, or if other parties to a transaction (e.g., a bank or insurance company) raise concerns, consult the Legal Department immediately. Know and watch for signs of suspicious behaviour, especially involving repeat counterparties.

Please refer to Appendix 2 Exhibit C for Red Flags.

4. TRANSACTIONS SUBJECT TO COMPLIANCE REVIEW

All potential counterparties of the Company will be subject to the compliance checks identified in this Policy based on a risk assessment.

Please refer to Part-B Section 2 for risk assessment.

Furthermore, the Company will routinely conduct compliance checks for existing counterparties to ensure that no current members of the Company counterparty base pose a compliance risk.

Whenever a new or existing customer or other relevant counterparty requests a change to the final shipment destination, the consignee involved, banking information, or other key transactional details, the relevant Managers or member of the Company Team must promptly notify the Legal Department and a new compliance check must be initiated based on the information received.

Please refer to Part-B for detailed procedure.

5. RECUSAL POLICY

5.1 General Summary of the recusal policy

Any person who is subject to the jurisdiction of a country other than India (a “**Third-Country Person**”) working for the Company is prohibited from participating in or approving any transaction directly or indirectly involving a person or entity targeted by such third country; if approved by the Legal Department, any function ordinarily performed by that Third-Country Person shall be performed by his or her supervisor or, if none, his or her deputy, or any other person designated by the head of the relevant department or unit.

The purpose of this recusal policy is to prevent the involvement of Third-Country Persons in any dealings that would result in a violation of any applicable non-Indian sanctions regime (“**Third-Country Sanctions**”).

You must contact the Legal Department if you are aware that Third-Country Sanctions are imposed on an entity or country, involved in a transaction, in order to ensure that any possible third country connection is identified and eliminated or licensed.

For the purposes of this policy, a Third-Country Person may be a Company Team member:

- a. with non-Indian citizenship (whether or not such person also has Indian citizenship);
- b. with permanent residence in a country other than India such as would subject that person to such country's sanctions regime; or
- c. any other person otherwise subject to the sanctions regime of a country other than India.

5.2 Application of Third-Country Sanctions while outside India

The Company Team must also bear in mind that anyone physically located in a country other than India, including temporarily, must comply with local law and must not participate in any business activity potentially involving applicable Third-Country Sanctions. Such a person is considered a Third-Country Person for the duration of his or her stay (for example, an Indian citizen on a business trip in London is subject to this recusal policy for transactions implementing UK sanctions while in London).

5.3 Recusal and Reporting Requirements

- a. No Third-Country Person may participate in any manner whatsoever in any business activity implicating Third-Country Sanctions applicable to such person, other than verifying that such a business activity complies with applicable Third-Country Sanctions law, and he or she has no authority to do so.
- b. The Company will not involve a Third-Country Person in a decision-making or management activity involving a business activity implicating Third-Country Sanctions applicable to such person, and will not assign such person to such business activity, except to ensure that such a business activity complies with applicable Third-Country Sanctions law.
- c. If a Third-Country Person ascertains that he or she is or may be involved in business activity that potentially implicates Third-Country Sanctions applicable to such person, such person must immediately cease such involvement and is required to:
 - notify other participants in the business activity that he or she is required to be recused and
 - immediately inform a supervisor who is not subject to such Third-Country Sanctions (or, if none, the Legal Department).
- d. If any person ascertains that he or she is involved in a business activity potentially implicating Third-Country Sanctions that has not previously been identified as such, the individual shall immediately inform a supervisor who is not subject to such Third-Country Sanctions (or if none, the Legal Department).
- e. Any covered person who is normally not a Third-Country Person but is temporarily located in a jurisdiction other than India (including on business or personal travel) will recuse himself or herself from, and may not participate in any way in any business activity identified as involving applicable Third-Country Sanctions during the duration of his or her stay.

5.4 No adverse impact

A disqualification or recusal made in good faith pursuant to this recusal policy shall not negatively affect a Third-Country Person's performance evaluation or deprive him or her of any employment opportunities that are not restricted by Third-Country Sanctions applicable to such person.

PART B: PROCEDURAL MANUAL

1. GUIDELINES FOR THE COMPANY TEAM

The Company Team is responsible for complying with the applicable provisions of trade sanctions and export control laws and this Policy. As a general rule, all employees have to comply with trade sanctions laws, and in particular, must:

- a. Refrain from funding or making available financial assets or economic resources for the benefit of Restricted Parties;
- b. Refrain from providing financial or other related services for the benefit of Restricted Parties;
- c. Comply with the provisions of applicable laws and this Policy at all times; this includes off-duty contacts insofar as the Company's interests are affected or employees are perceived by third parties to represent the Company;
- d. Raise any concerns as soon as possible, towards their respective direct manager, or the Legal Department, if he/she believes or suspects that a potential violation has occurred or may occur in the future; and
- e. Attend any training sessions or other events designed to communicate this Policy and updates to applicable laws and regulations.

“**Restricted Party or Parties**” here refers to mean a person that is (i) listed on any sanctions list or targeted by sanctions (whether designated by name or by reason of being included in a class of persons, including a party that operates in an industry subject to sectoral sanctions); or (ii) located in or incorporated under the laws of any country or territory that is the target of comprehensive, country-wide or territory-wide sanctions; or (iii) directly or indirectly owned or controlled by, or acting on behalf, or at the direction for the benefit of, a person referred to in (i) and/or (to the extent relevant under sanctions) (ii).

Be aware that if U.S. export controls are relevant to a particular transaction, in addition to restrictions that may apply to exports to the country in question, the U.S. Bureau of Industry and Security maintains several lists of persons to which exports, re-exports, or transfers may be restricted. Restrictions may also be imposed based on the end use of the item in the country in question.

2. RISK ASSESSMENT

The Company requires you to consider certain factors, including, but not limited to, listed below in relation to customers, third parties, enduse of goods and/or services, and end users/customers. Please note that the evaluation points for risk assessment in Sections 2.1. to 2.3. are merely indicative and are subject to relevant export controls/sanctions applicable at a given point in time or as determined by the Legal Department.

2.1 Counter-parties: customers and third parties

A company may be exposed to export control or economic sanctions risks due to interactions with customers as well as third parties, including but not limited to, supply chain entities/ persons, intermediaries engaged in a transaction, and banks or other financial institutions. The following risk factors must be taken into account for such customers and third parties:

- a. Have individuals and entities been checked against published sanctions and Specially Designated Nationals lists and other sanctions and export control lists?
- b. Do you have visibility into the controlling interests behind individual customers, suppliers or other third parties?
- c. Is the counter-party located in a country that is known for facilitating transactions on behalf of sanctioned countries, serving as a diversion point for sanctioned countries or regimes, or that is known as a location from which export controlled goods are improperly diverted?
- d. Is there a payment risk in relation to remittances to the bank of the counter-party?
- e. Does the country have an elevated corruption risk? (See [Transparency International Corruption Perceptions Index](#) to identify such countries).
- f. Is the counter-party operating in a sanctioned sector or high-risk sector, or in a sector that is particularly sensitive for relevant export control regimes?
- g. Will third parties, such as agents acting on your company's behalf or transporters moving your products, be involved in the transaction? Are there any restrictions on these third parties?

2.2 Product/service

Risk assessment for the shipment of products or the provision of services must be primarily assessed in relation to export controls. However, product or service-based risk assessments may also be relevant to analyses of economic sanctions risks if the product sold or service provided by the Company is related to a sector in which operation may expose the company to sanctions liability. A risk assessment should consider, for example, the following questions:

- a. Does the product or service you provide have a dual-use or military application?
- b. Is the product specifically restricted for export to the country of the customer or import from the country of origin?
- c. Is the product subject to controls based on the intended end use of the item?
- d. Does the product or service require an export license or license by a sanctions authority?
- e. Is the product or service subject to an embargo?
- f. Is this an allowable transaction under applicable sanction/ export controls?
- g. Are there any sanctions applicable to the location of the delivery?
- h. Is there a restriction on the currency usable to undertake the export (or re-export) or import of the product or service?

2.3 End-user details

- a. Have you confirmed the intended enduse of the product or services?
- b. Are there sanctions that might apply to that enduse or enduser?
- c. Can you verify whether the enduser and its ultimate beneficiary are subject to sanctions?
- d. Do you have an enduser statement and sanctions clause built into your sales contracts? (This is particularly important if the enduser is unknown)

3. **ROLE OF THE LEGAL DEPARTMENT**

The Legal Department is responsible for monitoring developments in international sanctions laws as well as educating sales officers, members of senior management, and other applicable employees, such as members of the finance and accounting teams, regarding sanctions compliance and the consequences associated with potential violations. The Legal Department shall identify such developments as needed and not less than once per year. In addition, the Legal and Compliance Department should cross-reference updates to applicable Sanctioned Persons and territories lists with the counterparty base of the Company and notify applicable members of the Company Team if dealings with a particular counter-party should be terminated.

The Legal Department is also responsible for overseeing the KYC process and ensuring that sales officers (or other applicable Company Team members) collect and submit the mandatory KYC information required from potential counterparties in advance of foreign/export sales, domestic sales with potential foreign end customers, transactions with foreign suppliers or other foreign counterparties, or transactions otherwise involving potential red flags (see **Appendix 2 Exhibit C**). Upon receiving the KYC documentation, the Legal Department must analyse the information received and screen the potential counterparties to determine whether the transaction may be undertaken. The Legal Department will maintain a database of documents and other information collected from the counterparties for the Company's reference including the third-party screening templates uploaded into the system, final third-party screening reports for counterparties, and any other relevant data or information pertaining to sanctions compliance.

The Legal Department may obtain access to any transactional records as needed to audit the compliance process and ensure that all necessary information has been obtained. The Legal Department is also responsible for reviewing and verifying transaction-related documentation and agreements/terms and conditions, including ensuring that such documents contain appropriate assurances before the underlying transaction may be executed.

If any potential counterparties refuse to or are unable to provide the mandatory KYC or transactional information, or if the KYC or transactional information received is false, the relevant Company Team member shall notify the Legal Department of the counterparty's explanation, and the Legal Department will be responsible for making a determination as to whether the transaction may proceed.

The Legal Department may consult with external legal counsel to determine the absence of red flags or in case of any clarifications that may be necessary with respect to any potential transactions.

4. QUARTERLY COMPLIANCE REPORTS

The Company Team members must submit a Quarterly Compliance Report regarding all new and existing counterparties subject to mandatory KYC collections in the preceding quarter to the Legal Department. The Legal Department shall evaluate this information and then archive and submit the Quarterly Compliance Report to the senior management for further review.

When elevating the Quarterly Compliance Report to senior management, the Legal Department must identify any inconsistencies observed within the submissions, any potential compliance risks, and any employees that may be liable for compliance violations.

In addition, the Legal Department should periodically test the effectiveness of the procedures outlined in this Policy (at least annually), such as by reviewing a random selection of export invoices to ensure that it has received all of the required information and that compliance checks were completed appropriately, interviewing Company Team members who submit inconsistent information related to a particular counter-party, or through other measures. Any determination regarding weaknesses in the Policy or proposed process improvements should be elevated to senior management.

5. IMPLEMENTATION OF THE COMPLIANCE POLICY

The Legal Department has authority to interpret and apply this policy. All the Company Team members should familiarise themselves with the portions of the Policy relevant to their functions.

The Company's Board is authorised to grant any exemptions subject to legal provisions for the time being in effect, where such exemption is necessary for business reasons, by passing an appropriate order recording such reasons, citing appropriate legal advice in this context for granting such exemption.

The Company's Board shall amend and update this Policy as per the applicable regulations from time to time.

The Company's Board may mandate the Company Team to attend requisite training sessions, seminars, held in respect of this Policy and ensure strict compliance thereof.

6. RECORD RETENTION

LML is committed to maintaining accurate and complete records in accordance with all applicable laws and regulations, including those related to economic sanctions and export controls. The Company Team under the supervision of the Legal Department shall maintain complete transaction documents and records, including all records on due diligence (such as correspondence with third parties via email, SMS (e.g., WhatsApp and Telegram); KYC forms and related correspondence; third party screening records; written records on due diligence results, etc.); records of correspondence submitted to the Legal Department regarding suspected, potential, or actual violations of sanctions or export control laws; and relevant compliance-related correspondence with third parties.

Document custody is crucial to the Company's compliance efforts. As prescribed by the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015, the Board of directors of a Company shall approve a policy for preservation of documents relating to any transaction such that the documents must be preserved for at least 8 years after the completion of the transaction.

International sanctions and export control laws require that transaction records be maintained for at least 10 years. Therefore, the Company must preserve all documents relating to any transaction for 10 years after the completion of the transaction.

7. TRAINING OF EMPLOYEES

The Company will provide training to its employees to increase risk awareness and to ensure compliance with this Policy and all relevant trade laws and regulations.

The Company's Legal Department, will design and implement an employee training plan to ensure that relevant employees, officers, representatives, and other applicable members of the Company Team (including members of the management, operations, sales, and finance teams) are regularly and appropriately trained on:

- a. Export control and sanctions laws and regulations, and in particular, KYC measures, detecting, and reporting of suspicious transactions;
- b. Prevailing techniques, methods, and trends in concealing the nature of transactions and/or beneficial owners so that applicable Company Team members can recognise any such red flags; and
- c. Internal policies, procedures, and controls related to export controls and sanctions, and the roles and responsibilities of employees, officers, representatives, and other applicable Company Team members.

Training sessions should provide job-specific knowledge (as needed), clarify the responsibilities of different classes of employees with illustrative examples, and include assessments that test employee knowledge, and which can be analysed to audit the training program itself and determine the necessity of additional sessions or other forms of employee-specific corrective action.

The Company may conduct additional training sessions or distribute updates to employees as needed. Situations where additional training or other company-wide communications may be warranted, include, for example, relevant changes in compliance laws and regulations, updates to industry-specific guidance or trends, or significant revisions to the Company's internal policies, procedures, or operations. Training sessions may be conducted with the aid of external legal counsel engaged by the Company.

8. QUESTIONS AND ESCALATIONS

If at any time you have reason to believe that the transfer of controlled items, shipment or receipt of any goods or services, or transactions related to goods or services, did not or does not comply with relevant export controls or sanctions laws, you must immediately halt all ongoing activity, if any, and report the matter to the Legal Department and the head of your concerned department. You should also halt all ongoing activity and notify the Legal Department if you are unsure whether the transfer of an item complies with relevant export controls or sanctions laws.

In case of any financial activity that may be subject to sanctions, such as, receipt or remissions of funds, insurance, processing of any invoices etc., it may be brought to the attention of the Legal Department. No financial activity suspected to be subject to sanctions risk may be undertaken without clearance from the Legal Department in writing, stating the reasons for the same.

Please contact the Legal Department if you have any questions about this Policy or about export controls or sanctions generally.

9. VIOLATIONS OF POLICY AND PROCEDURE

The Company takes seriously its obligations under applicable export control and sanctions laws. Employees who violate the provisions of this Policy and Procedure may be subject to disciplinary action, up to and including termination of employment.

Signature: _____

Name: Mullapudi Srinivas

Designation: Whole-time Director

PART C: APPENDICES

APPENDIX-1A: EXPORT CONTROL LAWS

Overview of Indian export controls

India maintains a harmonised list on export control of dual-use and military items, including software and technologies, having potential civilian/industrial applications as well as military and weapons of mass destruction use. It is restricted/permitted under an export authorisation or license (unless specifically exempted), except for certain items that are prohibited.

The relevant legislations include the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act of 2005, the United Nations (Security Council) Act of 1947, the Customs Act of 1962, the Foreign Trade (Development and Regulation) Act of 1992, the Arms Act of 1959, the Atomic Energy Act of 1962, the Chemical Weapons Convention Act of 2000, the Environment Protection Act of 1986, the Explosives Act 1884, etc.

India is a signatory to international conventions on disarmament and non-proliferation, viz., the Chemical Weapons Convention and Biological and Toxin Weapons Convention. It is also a member of the major multilateral export control regimes, viz., the Missile Technology Control Regime on missiles, delivery systems and related dual-use items, Wassenaar Arrangement on munitions/military items and Australia Group on Biological and Chemical items.

In consonance with the relevant control lists, guidelines and provisions of the international conventions, mechanisms and regimes, India regulates the exports of dual-use items, nuclear-related items, and military items, including software and technology under the Special Chemicals, Organisms, Materials, Equipment and Technologies (SCOMET) list, which is the National Export Control List of dual use items, munitions and nuclear related items, including software and technology.

For more information on Indian Export Control, please refer to <https://www.dgft.gov.in/CP/?opt=itchs-import-export>.

Overview of U.S. export controls

The United States imposes export controls to protect national security interests and promote foreign policy objectives related to dual-use items and less-sensitive military items through the Export Administration Regulations (“EAR”) (15 CFR Parts 730 – 774). The Bureau of Industry and Security (“BIS”) is responsible for regulating, implementing, and enforcing export controls for such dual-use items and less sensitive military items. Within BIS, Export Administration (“EA”) is responsible for processing license applications, counselling exporters, and drafting and publishing changes to the EAR; and Export Enforcement is responsible for compliance monitoring and enforcement of the EAR. BIS works closely with U.S. embassies, foreign governments, industry, and trade associations to ensure that the export, re-export and transfer (in-country) of items subject to the EAR is accomplished in compliance with the regulations.

BIS has developed a list of “red flags”, or warning signs, and compiled “Know Your Customer” guidance intended to aid exporters in identifying possible violations of the EAR. Both resources are publicly available, and their dissemination to industry members is highly encouraged to help promote EAR compliance. See [Supplement No. 3 to Part 732—BIS's “Know Your Customer” Guidance and Red Flags | Bureau of Industry and Security](#).

The EAR regulates transactions involving the export, re-export, or transfer (in-country) of “dual-use” and less sensitive military items (commodities, software, and technology) as well as certain U.S. person activities. The EAR also regulate exports, reexports, or in-country transfers of items

made in third countries that contain more than *de minimis* levels of U.S. content, and in specified situations the export, re-export, or in-country transfer of non-U.S. items that are the direct product of U.S. technology, or that are produced in a plant that is the direct product of U.S. technology.

While the EAR export control regime imposes the greatest level of controls on items specifically identified on the Commerce Control List (CCL), the EAR also imposes a lesser level of controls on items not specifically identified on the CCL. These items, which the EAR refers to as EAR99 items, need not have any dual use application at all. They are subject to restriction on export to terrorist supporting countries (Cuba, Iran, North Korea, and Syria), and may also be restricted for exports, re-exports, or in-country transfers to persons on the Entity List, or if intended for specific categories of end users or end uses.

For more information on US Export Control, please refer to <https://www.bis.gov/regulations>, and consult the Legal Department if you have any questions.

Overview of UK/EU export controls

All items listed by the Australia Group, Missile Technology Control Regime, Nuclear Suppliers Group, and Wassenaar Arrangement are subject to export control in the UK and EU. Both EU and UK implement the European Dual Use Export Control Annex.

The UK maintains a list of all items that are subject to strategic export controls. This is known as the consolidated list of strategic military and dual-use items that require export authorisation. The list includes items that are controlled because of international agreements or arrangements as well as further items relating to specific defence or security concerns of the UK. The two main categories of goods are (i) military goods, software and technology that are specially designed or modified for military use; and (ii) dual-use items which are goods, software and technology that can be used for both civilian and military applications.

Regulation (EU) 2021/821 governs the EU's export control regime, which includes common export control rules, a common EU list of dual-use items, common provisions for end-use controls on non-listed items, controls on brokering and technical assistance relating to dual-use items and their transit through the EU, specific control measures and compliance to be introduced by exporters, such as record-keeping and registers, and provisions for setting up a network of competent authorities supporting the exchange of information and the consistent implementation and enforcement of controls throughout the EU. In certain cases, EU Member States may introduce additional controls on non-listed dual-use items because of public security or human rights considerations.

For more information on UK export control, please refer to <https://www.gov.uk/guidance/uk-strategic-export-controls>

For more information on EU export control, please refer to <https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items-en>

APPENDIX 1B: SANCTIONS LAWS

Overview of Indian sanctions laws

India does not maintain an autonomous sanctions regime or a consolidated list of sanctions. However, India implements sanctions imposed by the United Nations (“UN”) through the United Nations (Security Council) Act, 1947 (“UNSCA”). Under the UNSCA, the Government of India is authorised to take any measures to give effect to any decision of the UN Security Council. This is done by notifying amendments to the applicable Foreign Trade Policy (“FTP”).

The Directorate General of Foreign Trade (“DGFT”), within the Ministry of Commerce and Industry of the Indian Government, is responsible for advising the Indian central government on the formulation of the FTP, which stipulates the sanctions regime in India. The DGFT is also responsible for carrying out the FTP and implementing the provisions of the relevant legislations. Further, in all matters relating to the interpretation of the FTP, the decision of the DGFT is final and binding.

Presently, India regulates trade with Iraq, Iran, North Korea, and Somalia and prohibits trade with organisations including Islamic State of Iraq and the Levant (ISIL, also known as Daesh), Al Nusrah Front and other individuals, groups, undertakings and entities associated with Al Qaida. India also maintains a list of terrorist organisations and individuals pursuant to the Unlawful Activities (Prevention) Act, 1967.

For a consolidated list of UNSC consolidated sanctions list, please refer to <https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list>.

Overview of U.S. sanctions

The United States maintains economic sanctions for national security and foreign policy purposes against a number of countries, persons, and entities. These sanctions may be primary or secondary. Primary sanctions apply to U.S. persons or activities with a U.S. nexus whereas secondary sanctions have a broader reach, applying to non-U.S. persons and activities without a link to the U.S..

Strict and complex requirements apply to any transaction involving, directly or indirectly, any person, entity, or country targeted by U.S. sanctions if the transaction has any connection whatsoever to the U.S., including:

- a. involvement of any U.S. person (any United States citizen, permanent resident alien, entity organised under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States);
- b. the procurement of goods or services (such as insurance or financing) from the U.S.;
- c. U.S. dollar payments; and
- d. any activity in the United States.

Non-U.S. persons are also subject to certain sanctions prohibitions such as causing or conspiring to cause U.S. persons to violate U.S. sanctions, as well as engaging in conduct that evades U.S. sanctions. Certain programs also require foreign persons re-exporting certain goods, technology, or services from the United States to comply with U.S. sanctions, even if no U.S. persons are involved in the re-export.

The U.S. Department of the Treasury's Office of Foreign Assets Control ("**OFAC**") is the primary agency responsible for the administration and enforcement of U.S. Sanctions Laws. The U.S. government administers and enforces more than 30 sanctions programs, and each contains different restrictions and measures. OFAC has three main methods to sanction or target countries, regions, entities, vessels, and individuals under its U.S. sanctions programs: (i) comprehensive sanctions, (ii) list-based asset blocking, and (iii) sectoral sanctions. Each type of sanction is briefly discussed below.

Comprehensive Sanctions

OFAC currently administers comprehensive economic sanctions against **Cuba, Iran, Syria, North Korea, and the Crimea, Donetsk, and Luhansk Regions of Ukraine**. In addition to the above programs, OFAC maintains an embargo on the **Government of Venezuela**, which subjects Venezuela to extensive sanctions.

The Company will not engage in any transactions or dealings with any counterparty located in a comprehensively sanctioned country, directly or indirectly (e.g., through agents, distributors, resellers, etc.), unless authorized under U.S. law and approved by the Company's Chief Executive Officer.

List-Based Asset Blocking

Sanctions target entities and individuals designated on OFAC's sanctions lists, including the Specially Designated Nationals and Blocked Persons List (the "**SDN List**").

Both SDNs *and entities in which they own 50% or greater stake* are "blocked", meaning that their assets in the United States or in the possession of U.S. persons are frozen, and U.S. persons are cut off from practically all transactions and dealings with them.

In addition to the embargoed countries listed above, OFAC's list-based country sanctions target SDNs relating to the following jurisdictions: **Afghanistan, Albania, Belarus, Bosnia and Herzegovina, Burma, Burundi, Central African Republic, Democratic Republic of the Congo, Ethiopia, Hong Kong, Iraq, Kosovo, Lebanon, Libya, Mali, Montenegro, Nicaragua, North Macedonia, Russia, Serbia, Somalia, Sudan, South Sudan, Ukraine, Yemen, and Zimbabwe**. These jurisdictions are generally higher-risk jurisdictions for sanctions compliance.

The Company may not do any business with any SDN or entity, owned 50% or more by SDNs.

Sectoral Sanctions

"Sectoral" sanctions target specific sectors of a country's economy. Currently, OFAC maintains sweeping sectoral sanctions against Russia, and other sectoral sanctions regarding Belarus.

Relevant to LML's line of business, the U.S. imposes broad sectoral sanctions on Russia's manufacturing industry. The U.S. authorizes sanctions on any entity, including foreign entities, that operate or have operated in the following sectors of the Russian Federation economy:

These sectoral sanctions are sweeping and prohibit many activities, even if there is no U.S. nexus to the transactions or business activities.

The United States defines operating in the manufacturing sector of the Russian Federation economy in a way that includes activities such as the creation, modification, repair, testing, or financing, of goods by manual labor or machinery involving the Russian Federation and any related activities, including the provision or receipt of goods, services, or technology to, from, or involving the manufacturing sector of the Russian Federation economy.

Due to sectoral sanctions directly related to the industries in which LML does business, the Company will not engage in any business with or connected to Russia, Belarus, or any country subject to sectoral sanctions, without the approval of the Company's Board.

For more information on US sanctions laws, please refer to <https://ofac.treasury.gov/>.

OFAC administers and enforces the sanctions program and maintains lists of Sanctioned Persons and entities.

To check whether an entity is sanctioned, please visit <https://ofac.treasury.gov/sanctions-list-search-tool> and [CSL Search](#). The fact that an entity or individual is not listed on the SDN list does not necessarily mean that engaging in business activities and transactions is permitted. You must also take into consideration applicable sectoral sanctions, as well as export control laws.

Overview of EU and UK sanctions

EU and UK sanctions do not apply to everyone on a worldwide basis. The following persons and activities are subject to EU and/or UK sanctions:

- a. EU or UK nationals, regardless of where they are living or working, as well as companies incorporated in the European Union or the United Kingdom;
- b. Any person or entity, to the extent, doing business (either in whole or in part) within the territory of the EU or UK; and
- c. Activities taking place within the territory of the EU or UK.

Mere use of the Euro or the British Pound does not generally subject the Company to compliance with EU or UK sanctions; however, the financial institutions involved in the transaction may be subject to such compliance, so EU and UK sanctions should be considered to avoid operational risks.

For more information on UK sanctions laws, please refer to <https://www.gov.uk/government/collections/uk-sanctions-regimes-under-the-sanctions-act>

and to check whether an entity is sanctioned please visit <https://www.gov.uk/government/publications/the-uk-sanctions-list>.

For more information on EU sanctions laws, please refer to https://www.eeas.europa.eu/eeas/european-union-sanctions_en.

and to check whether an entity is sanctioned please visit <https://data.europa.eu/data/datasets/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions?locale=en>.

APPENDIX 2

Exhibit A: Counter-party KYC information

A. KYC information for organisation (customer/supplier/other counterparty)

Organisation	
Organisation Name *	
Country Code *	
Address 1	
Address 2	
City	
State/Province Code	
Postal Code	
Category (Agent, Consultant, Contractor Distributor, Freight Forwarder, Joint Venture / Partner, Supplier, Vendor)	
Contract Amount *	
Start Date of Relationship *	
Ownership by a Public Official *	
Interacts with Government Entities *	
Third Party Payment Type	
Name of Third Party's Financial Institution	
Financial Risk *	
Approval Status * (New, In Process, Requires Additional Info, Requires Review, Approved, Approved with Qualifications, Denied, Terminated)	
Owner Email *	
Telephone No.	
Other Countries Where Active	
Transaction Final Destination	
Information on the Beneficial Ownership	
Additional Requested Information If Necessary	
Counterparty Unable to Provide Any Requested Information? If so, Please Explain	

B. KYC information for person (customer/supplier/other counterparty)

Person	
First Name *	
Middle Name	
Last Name *	
Country Code *	
Address 1	
Address 2	
City	
State/Province Code *	
Postal Code	
Current Employer	
Owner Email *	
Category (Agent, Consultant, Contractor Distributor, Freight Forwarder, Joint Venture / Partner, Supplier, Vendor)	
Contract Amount *	
Start Date of Relationship *	
Ownership by a Public Official *	
Interacts with Government Entities *	
Name of Financial Institution	
Financial Risk *	
Approval Status * (New, In Process, Requires Additional Info, Requires Review, Approved, Approved with Qualifications, Denied, Terminated)	
Telephone No.	
Other Countries Where Active	
Transaction Final Destination	
Counterparty Unable to Provide Any Requested Information? If so, Please Explain	

Exhibit B: LML's Standard Operating Procedure (SOP) for implementing the Policy

1. As set forth in the Policy for LML, before commencing any business, the relevant employee shall collect mandatory KYC information from all potential counterparties (whether entities or individuals) in sales involving foreign/export customers, domestic sales with potential foreign end customers, transactions involving foreign suppliers or other foreign counterparties, or transactions otherwise involving potential red flags, which is enclosed as **Appendix 2Exhibit C**, as well as trade mark registration details (if any), and any other supporting documents. Using a risk-based approach, it may be appropriate to collect additional KYC information in order to determine that no counterparties are acting on behalf of a sanctioned party, including but not limited to beneficial ownership information, the identity of directors, authorized signatories, and power of attorney holders (to the extent possible). If KYC information from any counterparties cannot be obtained, the Legal Department must be consulted in order to determine whether it is appropriate for the transaction to proceed.
2. The relevant employee shall ensure that all particulars of the collected KYC information are true and correct, inquire about other key transactional details (such as the contemplated end customers and final destination), and perform general online searches related to the counterparty to identify potential compliance risks. If a shipment requires further transit beyond the port of discharge, the relevant employee should ask the potential customer or other counterparties involved to provide assurances that the transaction does not involve any sanctioned territories, entities, or persons, including assurances that the counterparties involved are not owned, controlled by, or affiliated with any sanctioned parties.
3. The relevant employee shall share the collected KYC and other relevant information along with any supporting documents with the Legal Department for purposes of screening the counterparty, in order to identify any potential risks regarding sanctions compliance.
4. Upon receipt of the collected KYC information, the Legal Department will screen the counterparty using the third-party screening platform, which will generate a Report Score, and perform any other checks as deemed appropriate. This information will be circulated to the relevant employee and relevant department or unit head, who will work in consultation with the Legal Department to determine whether the transaction may proceed. KYC and other information related to new and existing counterparties will be maintained by the Legal Department including the third-party screening templates uploaded into the system, final third-party screening reports for counterparties, and any other relevant data or information pertaining to sanctions compliance.
5. Once the relevant business team members, upon approval of the Legal Department, deem it proper to conduct business with the relevant counterparties cleared of compliance concerns, the relevant employee shall enter into an agreement/contract/terms and conditions with the buyer/service provider/customer/contractor/other relevant party, but will ensure to include the separate Sanctions Clause (enclosed as **Appendix 2Exhibit D**).

The Company's proforma and commercial invoices shall further note that *"These goods are not intended for export directly or indirectly to sanctioned and/or embargoed countries, entities, or individuals, as designated by the U.S., UK, EU, UN or any other applicable international body"*.

6. Transactional documentation should be sent to the Legal Department in advance of execution so that the Legal Department can verify the proper assurances have been included and contracts may not be executed without final approval from the Legal Department.

7. Whenever a new or existing customer or other relevant counterparty requests a change to the final destination, the consignee involved, or other key transactional details, the relevant employee must promptly notify the Legal Department and a new compliance review must be initiated based on the information received. The presence of any other red flags or suspicious activity occurring after the initial compliance review should also be elevated to the Legal Department so that a new review may be instituted. Even after an existing customer has been cleared by the compliance review process, the Legal Department will review approximately 10% of the existing customer's export invoices approximately every six months to evaluate the counterparties involved and search for the presence of potential red flags.
8. In any transaction that requires KYC collection, repeat counterparties who have previously been approved by the Legal Department should still receive an updated third-party screening and any other checks as deemed appropriate by the Legal Department. If over one year has elapsed since mandatory KYC documentation has been collected from the counterparty, the Legal Department should direct the sales officer or applicable Company Team member to obtain updated KYC information from the counterparty, even if the counterparty represents that its KYC information has not changed.
9. If sales officers or any other relevant employees observe any potential violation or other compliance risk then they shall immediately notify the Legal Department. The Legal Department will review such information and notify senior management where appropriate. Disciplinary action will be taken in cases of non-compliance with the Policy and the appropriate authorities will be notified in the case of a sanctions violation.
10. Sales officers or other applicable Company Team members shall submit the Quarterly Compliance Report to the Legal Department for the business conducted during the preceding Quarter. The Legal Department shall review, archive, and submit this information, along with other relevant compliance-related updates, to senior management for review.
11. The Legal Department should periodically (and not less than once per year) test the effectiveness of the procedures outlined in the Policy, such as by reviewing a random selection of export invoices to ensure that it has received all of the required information and that compliance checks were completed appropriately, interviewing Company Team members who submit inconsistent information related to a particular counterparty, or through other measures. Any determination regarding weaknesses in the Policy or proposed process improvements should be elevated to senior management and all updates to senior management should be tracked and archived for potential future reference.
12. The Legal Department is responsible for monitoring developments in international export control and sanctions laws as well as educating sales officers, members of senior management, and other applicable employees, such as members of the finance and accounting teams, regarding sanctions compliance and the consequences associated with potential violations. Such updates will occur as needed and not less than once per year. In addition, the Legal Department should cross-reference updates to applicable Sanctioned Persons and territories lists with the Company counterparty base and notify the Company Team if contact with a particular counterparty should be terminated.
13. Sanctions training sessions should be developed that provide job-specific knowledge (as needed), clarify the responsibilities of different classes of employees with illustrative examples, and include assessments that test employee knowledge, and which can be analyzed to audit the training program itself and determine the necessity of additional sessions or other forms of employee-specific corrective action.

Exhibit C: Red flags

1. **Counterparties who attempt to provide insufficient or suspicious information:** A counterparty's reluctance to share essential details, such as identification, business activities, end-user information, or whether the product will be used domestically or re-exported, may indicate an attempt to obscure prohibited dealings or high-risk transactions. Additionally, it may be cause for concern if the customer provides a freight forwarding firm as the product's final destination.
2. **Similar Address or Name to Sanctioned Party:**The customer name or its address is similar to that of a person or entity found on a sanctions list such as the SDN List.
3. **Limited Business History or Track Record:** The customer has little or no business background and open-source searches reveal the company is newly-created or has no business or transaction history.
4. **Limited Knowledge:** The customer seems unfamiliar with the product's performance characteristics but still wants the product.
5. **Unexpected Changes:** The customer makes unusual (e.g., multiple or last-minute) changes to the order, such as requests to amend the port of discharge, switch payment methods, or to change the delivery address or information on bills of lading.
6. **Efforts to avoid reporting and recordkeeping:** Attempts to manipulate or bypass documentation requirements, such as altering invoices, avoiding regulatory oversight, or routing payments through unconventional channels, can signify an effort to evade sanctions compliance.
7. **Any activity inconsistent with counterparty's business:** Transactions that do not align with the counterparty's usual business operations or that involve unusual terms, products, or destinations may signal hidden or illicit intentions. Or, the product's capabilities do not fit the buyer's line of business, such as an order for a CNC machine for a small bakery.
8. The customer is willing to pay cash when the terms of sale would normally call for financing.
9. **Suspicious third-party involvement:** The involvement of unidentified or unusual third parties in payments or transactions, particularly without sufficient documentation, raises concerns about potential facilitation of prohibited activities.
10. **Any suspicious relationship with Government officials:** Close connections between a counterparty and government officials, especially those recently in office or involved in recommending intermediaries, can indicate corruption risks or undue influence.
11. **Potential involvement of high-risk territories, persons, or end-users:** Transactions involving sanctioned regions, entities, or individuals, either directly or through transit routes known for sanctions violations, require additional scrutiny to avoid compliance breaches.
12. **Other suspicious activities:** Unusual patterns, such as abnormal shipping routes, or products appearing in black markets or at unreasonably low prices, can indicate diversion to unauthorised or prohibited recipients.

13. **Involvement of Sanctioned or Otherwise High-Risk Countries:** You know or suspect that the transaction or business activity is related to a sanctioned or otherwise high-risk country. This does not necessarily mean that the entity is registered in a country subject to sanctions (whether a complete embargo/comprehensive sanctions or sectoral or other sanctions) or an embargo. This can also mean that there is *any* connection whatsoever to a high-risk country. Sanctioned, embargoed, or otherwise high-risk countries include Russia, Belarus, certain regions of Ukraine, Syria, Cuba, Venezuela, Iran, and certain regions of Ukraine. **NOTE:** LML does not do business or engage in any transactions with Russian entities or individuals. If you think there is a connection (direct, indirect, hidden or otherwise) to Russia, you **must** consult the Legal Department.

Exhibit D: Sanctions compliance clauses for agreements/contracts

Following are some indicative sanctions compliance clauses that may be utilised while drafting agreements/contracts:

- (a) *Neither the Counterparty nor any of its Beneficial Owners or Subsidiaries, nor any of their respective directors, officers, employees nor, to the knowledge of the Counterparty, any persons acting on any of their behalf is:*
 - (i) *A Sanctioned Person; or*
 - (ii) *Has received notice of or is aware of any claim, action, suit, proceeding or investigation against it with respect to Sanctions by any Sanctions Authority.*
- (b) *The Counterparty represents and warrants that it will not, directly or indirectly, deal with any Sanctioned Person or Sanctioned Territory in connection with this Agreement or the products or services to be supplied hereunder, nor will it violate or cause the Company to violate any Sanctions in connection with this Agreement or engage in any other manner that would reasonably be expected to result the Company being in breach of any Sanction or becoming a Sanctions Person.*
- (c) *Neither the Counterparty, nor any of its Subsidiaries shall engage in any transactions or activities that evades or avoids, or has the purpose of evading or avoiding, or breaches or attempts to breach, whether directly or indirectly, any Sanctions.*

Definitions

“Sanctioned Territory” means any country or territory with which dealings are broadly and comprehensively prohibited by any country-wide or territory-wide Sanctions (as of the date hereof, North Korea, Cuba, Iran, Syria, and Crimea).

“Sanctioned Person(s)” means any Person with whom dealings are restricted or prohibited under any Sanctions, including as a result of that Person’s: (a) being named on any list of Persons subject to Sanctions, (b) being located, organised, or resident in, or directly or indirectly owned or controlled by the government of, any Sanctioned Territory, or (c) having any direct or indirect relationship of ownership, control, or agency with a Person described in (a) or (b).

“Sanctions” means all laws and regulations of India, the United States, the United Kingdom, or the European Union, or United Nations Security Council resolutions, concerning economic sanctions, embargoes, or the freezing or blocking of assets or transactions of targeted Persons, OR

“Sanctions” means the economic sanctions laws, regulations, embargoes or restrictive measures administered, enacted or enforced by: (a) the United States government; (b) the United Nations; (c) the European Union or any member state of the European Union; (d) the United Kingdom; (e) Singapore; (f) Japan; (g) the French Republic; or (h) the respective governmental institutions and agencies of any of the foregoing, including, without limitation, the Office of Foreign Assets Control of the US Department of Treasury (“**OFAC**”), the United States Department of State, His Majesty’s Treasury (“**HMT**”), the Monetary Authority of Singapore, the Ministry of Finance, Japan, the Ministry of Foreign Affairs of Japan and the Japan Financial Services Agency and/or any other applicable jurisdiction (together the “**Sanctions Authorities**”).

Sanctions List means the "Specially Designated Nationals and Blocked Persons" list maintained by OFAC, the Consolidated List of Financial Sanctions Targets and the Investment Ban List maintained by HMT, or any similar list maintained by, or public announcement of Sanctions designation made by, any of the Sanctions Authorities.