ESR Group Limited
(Stock code: 1821)

ANTI-MONEY LAUNDERING, COUNTER-TERRORIST FINANCING & SANCTIONS

OWNER: GROUP COMPLIANCE

CONTENTS

1. INTRODUCTION

1.1 ESR Group Limited and its subsidiaries (collectively, "**ESR**" or the "**Group**") are committed to putting in place effective policies and procedures to address the anti-money laundering ("**AML**"), counter-terrorist financing ("**CTF**"), and sanctions compliance requirements of its business units ("**Business Units**") in conducting businesses and operations, particularly with a focus on the potential counterparties of our Group.

1.2 A counterparty may include any person or entity on the other side of a transaction in which the Group is involved, such as capital partners/investors, sellers or buyers of real assets, Joint Venture partners, suppliers and any other party that participates in a financial transaction with the Group.

1.3 Money laundering, terrorist financing, and violation of sanctions are **criminal offenses** under many countries' local laws. For instance, under Hong Kong's United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575) ("**UNATMO**"), it is an offence for a person to provide or collect funds knowing or with the intention that the funds will be used for terrorism.

1.4 Money laundering and terrorist financing manipulations are similar, as both are associated with the concealment and disguise of benefits derived from criminal conduct. Money launderers will send the proceeds of crime through legal channels to conceal their criminal origin, while financiers of terrorism will transfer funds, which may be legal or illegal, to conceal the source and ultimate use, i.e., the support of terrorism.

1.5 Given that the AML/CTF and sanctions regulations may differ among the jurisdictions in which the Group has business operations, where a conflict arises between the Group Anti-Money Laundering, Counter-Terrorist Financing & Sanctions Policy (the **"AMLCTF & Sanctions Policy"**) and the local AMLCTF & Sanctions Policy, please refer to your local compliance officer for further clarification. For the avoidance of doubt, the more restrictive provision will apply.

2. PURPOSE AND SCOPE

2.1 This policy outlines the regulatory requirements for AML/CTF and sanctions compliance and is addressed to business partners (if applicable), directors, employees (part-time or full-time,

permanently or temporarily employed), secondees, interns and officers (together, "**Employees**") who undertake roles on behalf of the Group. This policy may apply to contractors, consultants who are engaged to work under the supervision, direction, or control of the Group and such other persons as determined by the local compliance officer (who have notified these third parties in writing) as being within the scope of this policy.

2.2 The Financial Action Task Force ("**FATF**") is an international inter-governmental body that sets standards and promotes AML/CTF measures. It has issued the Recommendations ("**R**s") as a framework to detect and prevent money laundering and terrorist financing ("**ML/TF**") activities. The Rs are important and used as the basis of, or as a reference for, legislation and regulation in many jurisdictions around the world. Although FATF is aimed at financial institutions, the Rs are nevertheless made reference to by many non-banking corporations. In all the countries the Group currently operates, all of them are the members of FATF and the local financial institutions are required to implement the Rs that indirectly have an impact to our Group when we conduct our businesses (please refer to http://www.fatf-gafi.org/home/).

2.3 For details on the statutory definition and relevance of Money Laundering and Terrorist Financing ("ML/TF"), please refer to **Appendix A** for more information.

3. AML/CTF/SANCTIONS MANAGEMENT

3.1 Senior Management

Senior management is responsible for the oversight of the AML/CTF/sanctions systems and ensuring that the systems are capable of addressing the ML/TF/sanctions risks identified. The key persons involved in the management of the AML/CTF/sanctions systems and controls are the Compliance Officers ("**COs**"), and if applicable, the Money Laundering Reporting Officer ("**MLRO**") and, in respect of Cayman Islands operations, the Deputy Money Laundering Reporting Officer ("**DMLRO**"). Where necessary, ESR may delegate these functions to ensure compliance with its obligations under the applicable AML/CTF/sanctions regime. Where such functions are delegated, ESR will ensure all documentation and appropriate arrangements are put in place and remain ultimately responsible for ensuring compliance with its own AML/CTF/sanctions obligations.

3.2 Compliance Officer

COs encompass both the group compliance and the local compliance officers. The COs are responsible for the oversight of all activities relating to the prevention and detection of ML/TF/sanctions and providing support and guidance to the senior management to ensure that ML/TF/sanctions risks are adequately managed. The local compliance officer is responsible for discharging their duties and performing ML/TF/sanctions due diligence on any counterparty to comply with their local regulatory requirements. In addition, group compliance has oversight of the counterparty risk management and can assist to perform due diligence on any counterparty with whom the Group enters into a business relationship by gathering information on the counterparty and taking into consideration the risks, costs and services available.

3.3 Money Laundering Reporting Officer (if applicable)

MLRO should play an active role in the identification and reporting of suspicious transactions. The MLRO should receive, consider and investigate reports in respect of any information or matter which gives rise to actual knowledge or suspicion of money laundering, terrorist financing, or a breach of applicable sanctions. The MLRO should be your local compliance officer or one from the group office if there is no such local person.

In respect of operations connected with the Cayman Islands, a DMLRO's role is to act as the MLRO in the absence of the MLRO (references in this policy to the MLRO include the DMLRO in the absence of the MLRO).

3.4 Human Resources ("HR")

Staff screening procedures are put in place to ensure the integrity of any new employees, appointing officers and representatives, and the HR department or responsible staff should liaise with compliance on such screening reports.

4. RISK-BASED APPROACH ("RBA") AND DEFINITIONS

4.1 ESR adopts the risk-based approach in combating ML/TF and sanctions violations. This includes taking steps appropriate to the size, nature and complexity of the business to identify, assess and understand its ML/TF/sanctions risks.

4.2 Having undertaken this assessment and determining the level of risk, appropriate levels and types of mitigation will be applied and the risk assessment will be kept current through on-going reviews and monitoring.

4.3 The general principle of a RBA is where counterparties are assessed to be of higher ML/TF/sanctions risks, enhanced measures should be taken to manage and mitigate those risks, and correspondingly where the risks are lower, simplified measures may be applied. This will ensure that resources are being allocated in the most efficient way in accordance with priorities so that the greatest risks receive the highest attention.

4.4 Definition of **Ultimate Beneficial Owners** ("**UBO**")

The ultimate beneficial owner in relation to a counterparty means the natural person who:

(a) ultimately owns or controls, directly or indirectly, including through a trust or bearer share holding in accordance to the stipulated percentage based on the local regulatory or jurisdiction requirements of the voting rights at general meeting or the issued share capital of the corporation; or

(b) exercises ultimate effective control over the management of the corporation, a legal person or legal arrangement.

It is the responsibility of the local compliance team or transaction team to perform the necessary background check of the counterparties and UBO in accordance with the local regulatory, jurisdictions or business requirements. In some circumstances, for sanctions purposes it may be necessary to check ownership details even if they fall below the thresholds set above.

4.5 Enhanced Due Diligence **("EDD")** and more stringent on-going monitoring measures should be applied on **medium/high-risk counterparties**, such as an individual (or corporate entity) whose Source of Wealth ("**SOW**") and Source of Funds ("**SOF**") are to be determined or who requires the setting up of complex ownership structures.

4.6 Central to the RBA is the ML/TF Risk Assessment on the counterparty which involves identifying and categorizing ML/TF risks at counterparty level so that reasonable measures based on risks identified can be developed to effectively manage the corresponding risks. In

determining the ML/TF risk profile of a particular counterparty, relevant factors may include country risk and counterparty risk.

4.7 On-going Review

The identification of high-risk counterparties and geographical locations are not static assessments. They will change over time, depending on how circumstances develop, and how threats evolve. In addition, while a risk assessment should always be performed at the inception of a counterparty relationship, for some counterparties, a comprehensive risk profile may only become evident once the counterparty has begun transacting through an account, making monitoring of counterparty transactions and on-going reviews a fundamental process of RBA.

5. COUNTERPARTY ML/TF RISK ASSESSMENT

5.1 Counterparty ML/TF risk assessment is an important process to evaluate the ML/TF risk of counterparty, based on the objective information, documents and observation. Assessment of counterparty's ML/TF risk must be documented and recorded with any high-risk factors identified and considered.

5.2 For institutional/corporate counterparty, the risk assessment shall consider the business profile of the account holder and, if applicable, its connected company(ies) (e.g. parent, subsidiary or sister companies) and its connected person(s) e.g. the authorized persons/signatories, directors, shareholders, partners, ultimate beneficial owners.

5.3 For individual counterparty, the risk assessment shall consider the personnel profile of the account holder and the authorized person(s) (if any).

5.4 Under normal circumstances, it is the Group's policy NOT to receive and pay any third-party names other than the counterparty's own name. Any exception needs to be well supported by evidence for local compliance's approval for exceptional handling. Group compliance will circulate AML/CTF & sanctions-related regulatory news on updated lists of sanctioned names under relevant rules and regulations for any necessary screening purpose from time to time.

5.5 Under the CDD requirements and processes, the counterparty ML/TF risk assessment should be completed at the outset of the business relationship, annual review for high-risk counterparty and upon trigger event where there are changes in circumstances for low-risk counterparty.

6. COUNTERPARTY DUE DILIGENCE ("CDD") PROCESS

6.1 CDD is a baseline procedure performed by the Business Units in gathering the counterparties' background information and supporting documents which are submitted through the compliance risk management and due diligence platform. Reasonable steps are taken to establish the true and full identity of each of the counterparty, ascertain the risk level and carry out the appropriate due diligence response.

6.2 In layman terms, **Know-Your-Customer ("KYC")** is concerned with "knowing" enough about the counterparty by effective means and the processes on the obligation of CDD/KYC will arise in the following circumstances:

(a) at the outset of a business relationship;
(b) when there is a suspicion that the counterparty or their account or transaction is involved in ML/TF; or
(c) when there are doubts on the veracity or adequacy of any information previously obtained for the purpose of identifying the counterparty or for the purpose of verifying the counterparty identity.

7. SIMPLIFIED OR ENHANCED COUNTERPARTY DUE DILIGENCE ("SDD" or "EDD") PROCESS

7.1 SDD means that application of full CDD measures is not required. In practice, this means that the CDD process is completed, when the identification and verification of the counterparty and its ultimate beneficial owner are collected and submitted through the compliance risk management and due diligence platform which produces a low final risk rating and screening result.

7.2 SDD must not be applied under the following situations:

(a) When there is knowledge or suspicion that the counterparty's account or the transaction

is involved in ML/TF or there is increased risk that this is the case;

(b) When there is any doubt on the veracity or adequacy of any information previously obtained for counterparty identification.

7.3 Where the counterparty is assessed to be of higher risk, the following EDD procedures shall apply:

- Inform both the local and group compliance officers;
- Obtain higher approval through the compliance risk management and due diligence platform;
- Determine and document the source of fund/wealth of the counterparty (also for PEP, if applicable), and
- Place the counterparty on watch list and monitor all transactions with the counterparty.

In general, a PEP is defined as:

i) an individual who is or has been entrusted with a prominent public function in a place within (for domestic PEP) or outside (for foreign PEP) the country and includes a head of state, head of government, senior politician, senior government, senior judicial or military official, senior executive of a state-owned corporation, senior political party official and senior management of international organizations[3];

ii) a spouse, a partner, a child (step-child, adopted child), sibling (step-sibling, adopted sibling) or a parent (step-parent) of an individual falling within subparagraph i) above, or a spouse or a partner of a child of such an individual; or

iii) a close associate of an individual falling within subparagraph i above.

7.4 Note: If deemed necessary, the Business Units may conduct further background check through proprietary database; or appoint a qualified external intermediary to conduct due diligence on the counterparty (and ultimate beneficial owner, if applicable). The result of this further background check shall form the basis for higher approval in the compliance risk management and due diligence platform.

8. ON-GOING MONITORING

8.1 It is important to conduct on-going monitoring of counterparties to minimize the ML/TF

[3] International organization means an entity established by formal political agreements between member countries or jurisdictions that have the status of international treaties, whose existence is recognized by law in member countries or jurisdictions and which is not treated as a resident institutional unit of the country or jurisdiction in which it is located.

exposure of ESR.

8.2 The extent of monitoring should be linked to the risk profile of the counterparty which has been determined through the risk assessment. To be most effective, resources should be targeted towards business relationships presenting a higher risk of ML/TF. On-going monitoring of low risk counterparties include monitoring of any subsequent material changes to the initial information collected about the counterparty (e.g. change in ultimate beneficial owners or nature of business) or as part of the day-to-day operations of the Business Unit that identified a trigger event For high-risk counterparties, on-going monitoring is required to be performed annually, where such counterparties information is submitted through the compliance risk management and due diligence platform for screening at the end of each year.

8.3 Any findings and outcomes of the examinations related to on-going monitoring activities that have raisedany suspicions, proper records should be well documented in writing and consider the filing of a suspicious transaction report. Particular attention should be paid for unreasonable or unsupported transaction or third-party transfer requests.

9. SUSPICIOUS TRANSACTION REPORTING ("STR")

9.1 CDD and on-going monitoring provide the basis for recognizing unusual and suspicious transaction and events. An effective way of recognizing suspicious activity is knowing enough about the counterparties, their circumstances and their normal expected activities to recognize when a transaction or instruction, or a series of transactions or instructions, is unusual.

9.2 Whenever there is a **knowledge or suspicion** of ML/TF, employees are obligated to report to the Money Laundering Reporting Officer ("MLRO") (or DMLRO as applicable) as soon as reasonable. The obligation to report applies regardless whether or not a transaction is actually conducted, i.e. whenever a suspicion arises without reference to transaction per se. The MLRO (or DMLRO if applicable) will further review and may further enquire and gather additional information to determine whether or not it is necessary to make a report to the respective local regulator (if required by law) in light of all available relevant information. The filing from the reporting employee and to the regulator are all kept under **confidential basis** and **no one is allowed to disclose** to any other persons that may prejudice potential subsequent investigation. Any funds/financial assets of the suspected counterparty will be

frozen in accordance with the relevant legislation and court order.

Group compliance shall document all transactions that have been brought to the attention of the AML/CTF function including transactions not reported to the regulatory bodies and the basis for not submitting the STRs.

10. SANCTIONS

10.1 Full Commitment to Sanctions Compliance & Scope

The sanctions landscape is constantly changing and growing increasingly complex, creating legal and compliance risks for the Group, its management, and its Employees. Typically, sanctions issues are highly fact-sensitive. Breaching sanctions regulations may amount to an administrative infraction and/or a criminal offence, punishable by fine or, for individuals, even imprisonment.

ESR is committed to conducting all its business in full compliance with applicable sanctions regulations in all markets in which it operates, and has the management's complete support in this endeavor. The RBA that the Group has put in place for the purposes of AML/CTF compliance shall also inform the Group's approach to sanctions compliance. Unless otherwise provided in or modified by this section 10, the principles governing ML/TF due diligence shall apply *mutatis mutandis* to sanctions due diligence.

All Employees are required to strictly abide by the terms of this policy, which applies to all functions of the Group.

The Group's subsidiaries and local offices shall adopt and implement sanctions policies adapted to local requirements. Where there is a conflict between this Group policy and a local policy, the most restrictive provisions shall apply.

10.2 Violations of Sanctions Policy

(a) Doing business in violation of applicable Sanctions Measures could lead to negative legal, commercial and reputational consequences for ESR and/or for individual Employees, including civil liability and even criminal penalties. By adhering to the

terms of this policy, Employees help to ensure that such negative consequences are avoided.

(b) Disciplinary action (including dismissal) may be taken against any Employee who:

(i) Authorizes or participates directly in a violation of this policy;
(ii) Deliberately fails to report a violation, or suspected violation, to his manager or local compliance officer;
(iii) Deliberately withholds information, documentation or other material relevant to a violation or suspected violation;
(iv) Fails to cooperate with an investigation into a violation or suspected violation;
(v) Retaliates against anyone who has raised a concern about a violation or suspected violation;
(vi) In their capacity as manager or supervisor, displayed negligence or a serious lack of oversight/supervision having led (or contributed to) a violation.

(c) A person found or suspected to have violated the terms of this policy may in an appropriate case be referred to the relevant authorities, whether or not disciplinary action is also taken against them.

11. RECORD KEEPING

11.1 Under the Group's Code of Conduct and Business Ethics Policy for record keeping purpose, it is necessary to maintain counterparty, transaction and other records to ensure that:

(a) the audit trail for the movement of funds that relate to any counterparty and where appropriate, the ultimate beneficial owner of the counterparty, account or transaction is clear and complete;
(b) any counterparty and where appropriate, the ultimate beneficial owner of the counterparty can be properly identified and verified;
(c) all counterparties and transaction records and information are available on a timely basis to regulatory authorities, other authorities and auditors; and
(d) all records, including, records of counterparty's ML/TF risk assessment, registers of suspicious transaction reports and staff training records should comply with the record-

keeping requirements.

11.2 Period of Record Keeping

The form where records of document, data or information should be kept can either be in original copy, copy of the document, on microfilm, or in the database of computer.

(a) Subject to local law requirements, records relating to a counterparty should be kept throughout the business relationship with the counterparty and for a period of **6 years (or any** minimum period as stipulated by local regulations) following termination of the business relationship.

(b) Subject to local law requirements, records relating to a transaction should be kept for a period of **6 years (or any minimum period as stipulated by local regulations)** following the completion of a transaction, regardless of whether the business relationship ends during the period.

(c) Where the records are relevant to an on-going criminal or other investigation or any other purposes as specified in a notice served by the relevant authority, the records may be required to be kept for a period longer than those specified under (a) and (b) above.

12. STAFF TRAINING AND EDUCATION

12.1 Training on anti-money laundering, anti-terrorist financing and sanctions will be provided for new employees via e-learning course assigned to ensure that they are aware of their personal obligations under the relevant legislation and guidelines and that they can be personally liable should they fail to report as required.

12.2 Refresher training will be provided regularly to generate and maintain a level of awareness and vigilance to enable suspicious transactions to be recognized and reported.

12.3 Records of relevant training materials used and attendance by the participants will be maintained in the e-learning system or kept by Compliance for any external courses enrolled and completed.

APPENDIX A: MONEY LAUNDERING AND TERRORIST FINANCING

1.1 Money Laundering ("ML")

Money laundering is the generic term used to describe the process by which criminals disguise the **original ownership** and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a **legitimate source**.

Different jurisdictions define crime **predicating** the offence of money laundering in different ways. Generally, the differences between the definitions may be summarized as follows:

a) Differences in the **degree of severity** of crime regarded as sufficient to predicate an offence of moneylaundering. For example, in some jurisdictions it is defined as being any crime that would be punishable by one or more years imprisonment. In other jurisdictions the necessary punishment may be three or five years imprisonment; or

b) Differences in the **requirement for the crime to be recognized** both in the country where it took placeand by the laws of the jurisdiction where the laundering activity takes place or simply a requirement for the conduct to be regarded as a crime in the country where the laundering activity takes place irrespective of how that conduct is treated in the country where it took place.

In practice almost **all serious crimes**, including, drug trafficking, terrorism, fraud, robbery, prostitution, illegal gambling, arms trafficking, bribery and corruption are capable of predicating money laundering offences in most jurisdictions.

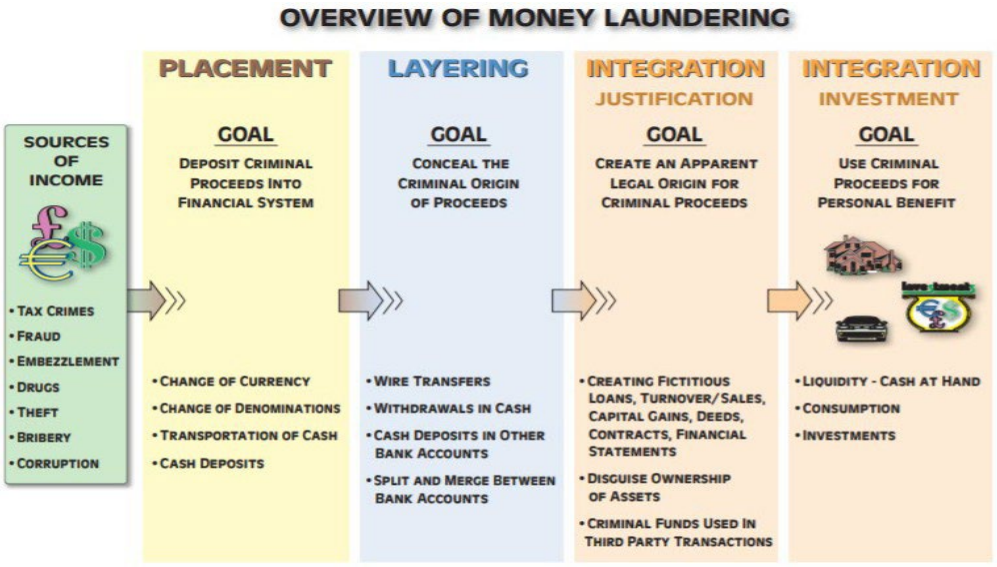
1.2 Stages of ML

Money laundering is generally identified as having three stages which are:

a) **Placement** – the physical disposal of cash proceeds derived from illegal activities;

b) **Layering** – separate illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of the money, subvert the audit trail and provide anonymity;

c) **Integration** – creating the impression of apparent legitimacy to criminally derived wealth. In situation where the layering process succeeds, integration schemes effectively return the laundered proceeds back into the general financial system and the proceeds appear to be the result of, or connected to, legitimate business activities.



1.3 Potential Uses of the Securities, Futures Contracts or Leverage Foreign Exchange Contracts (collectively referred as "securities businesses") in the ML Process

The securities businesses are more likely to be used at the second stage of money laundering, i.e. the layering process. Unlike laundering via banking networks, these businesses provide a potential avenue which enables the launderer to dramatically alter the form of funds. Such alteration may not only allow conversion from cash in hand to cash on deposit, but also from money in whatever form to an entirely different asset or range of assets such as securities or futures contracts, and, given the liquidity of the markets in which these instruments are traded, with potentially great frequency.

1.4 Terrorist Financing ("TF")

"Terrorist financing" is the financial support of terrorism or those who encourage, plan, or engage in terrorism. Terrorists or terrorist organizations require financial support in order to achieve their aims. "Terrorist financing" includes the financing of terrorist acts, and of terrorists and terrorist organizations. This generally entails the carrying out of transactions involving funds owned by terrorists, or which have been, or are intended to be, used to assist in the commission of terrorist acts. There is often a need for terrorists

to obscure or disguise links between them and their funding sources. It follows then that terrorist groups must similarly find ways to launder funds, regardless of whether the funds are from a legitimate or illegitimate source, in order to be able to use them without attracting the attention of the authorities.

1.5 How are Efforts to Combat Money Laundering and Financing of Terrorism linked?

Money laundering is the process of concealing the illicit origin of proceeds of crimes. Terrorist financing is the collection or the provision of funds for terrorist purposes. In the case of money laundering, the funds are always of illicit origin, whereas in the case of terrorist financing, funds can stem from both legal and illicit sources. The primary goal of individuals or entities involved in the financing of terrorism is therefore not necessarily to conceal the sources of the money but to conceal both the funding activity and the nature of the funded activity.

Similar methods are used for both money laundering and the financing of terrorism. In both cases, the actor makes an illegitimate use of the financial sector. The techniques used to launder money and to finance terrorist activities/terrorism are very similar and, in many instances, identical. An effective anti-money laundering/counter-terrorist financing framework must therefore address both risk issues: it must prevent, detect and punish illegal funds entering the financial system and the funding of terrorist individuals, organizations and/or activities. Also, AML/CTF strategies converge; they aim at attacking the criminal or terrorist organization through its financial activities, and use the financial trail to identify the various components of the criminal or terrorist network. This implies to put in place mechanisms to read all financial transactions, and to detect suspicious financial transfers.

Document Title	Anti-Money Laundering, Counter-Terrorist Financing & Sanctions
Document Language	English
English Title	Anti-Money Laundering, Counter-Terrorist Financing & Sanctions
Category	Group Policy
Policy Producing Function	Group Compliance
Document Author	Group Compliance
Document Approver	BOD
Portfolio Owner	Group Compliance
Original Issue Date	16 March 2018
Last Review Date	22 March 2023
Frequency of Review	Annually (or as required)
Version	1.4