LISI GROUP (HOLDINGS) LIMITED

利時集團(控股)有限公司

(a company incorporated in Bermuda with limited liability)

(stock code : 526)

(the "**Company**")

ANTI-MONEY LAUNDERING POLICY

(Adopted by the Company pursuant to the board resolution passed on 16 June 2026)

1. Purpose

1.1 The Company and its subsidiaries (collectively, the "Group") are committed to upholding high standards of business ethics and corporate governance and in compliance with all relevant anti-money laundering ("AML") and applicable laws and regulations in Mainland China, China Hong Kong and the jurisdictions in which the Group operates.

1.2 Doing business in violation of AML laws could lead to civil or criminal penalties and significant reputational risks for the Company. Employees and other persons connected to the Company could also face civil or criminal penalties.

1.3 The purpose of this Anti-Money Laundering Policy ("Policy") is to set out the main areas of money laundering risks facing the Company and the principles that the Company applies to comply with applicable AML laws. The Company has adopted this Policy to help its employees comply with these anti-money laundering requirements and applicable AML laws.

2. Scope of Application

2.1 This Policy applies to all employees, including employees at all levels and others who may act on behalf of the Group. Employees should familiarise themselves with this Policy. Failure to adhere to this Policy may result in disciplinary action (which may include summary dismissal) and/or referral to law enforcement.

3. Definition of Money Laundering

3.1 Money laundering is the criminal practice of handling or possessing criminal property, which is a benefit a person receives from criminal conduct. Criminal property can include money, securities, tangible property or intangible property. Money laundering does not necessarily involve cash or cash equivalents at every stage of the laundering process.

3.2 Money laundering can be a very simple process. For example, a person uses money raised from an illegal activity to purchase a clean asset, and in doing so, distancing the benefit of the illegal activity from the illegal activity itself, and enabling the launderer to enjoy the benefit of his crime.

3.3 Money laundering can also be highly complex. Most complex money laundering schemes follow three stages that may occur separately or simultaneously in order for money laundering to occur:

(i) **Placement** is the initial placement of illegally-derived (criminal) money into a legitimate financial context (usually with the aim of avoiding the attention of financial institutions or law enforcement). For example, profits derived from a corruptly procured contract, which are mixed with untainted funds a company holds.

(ii) **Layering** involves the distancing of illegal proceeds from their criminal source through the creation of layers of financial transactions, for example, via offshore companies. Possible examples of layering include unnecessary currency exchange, exchanging monetary instruments for larger or smaller amounts or wiring or transferring funds to and through numerous accounts in one or more financial institutions.

(iii) **Integration** occurs when the criminal money ultimately becomes absorbed into the economy in a way that appears to have been derived from a legitimate source, for example by investing that money.

4. AML Systems

4.1 To fulfil the obligations to mitigate the risk of money laundering and ensure legal compliance under the AML laws, the Group should assess the risk of the businesses, develop and implement policies, procedures and controls (collectively, "AML systems") on:

(a) risk assessment;
(b) customer/counterparty due diligence ("CDD") measures;
(c) ongoing monitoring of customers/counterparties;
(d) suspicious transactions reporting;
(e) record keeping;
(f) staff training; and
(g) independent audit function.

4.2 The Group establishes and implements adequate and appropriate AML systems (such as business relationship acceptance policies and procedures) taking into account factors including, *inter alia*, products and services offered, types and level of risks of customers/counterparties and geographical locations involved. This is to ensure the AML systems can address the money laundering risks identified.

4.3 Risk Assessment

(a) The Group adopts a risk-based approach to identify, assess and take action to mitigate money laundering risks. Control and oversight adopted, including the extent of CDD, the level of ongoing monitoring and the risk mitigation measures, should be appropriate in view of the customer/counterparty's money laundering risks identified.

(b) In determining the money laundering risk rating of a customer/counterparty, the Group considers a range of risk factors relevant to the specific circumstance. The following factors may be considered:
(i) Country/geographic risk
(ii) Customer risk
(iii) Product/service risk
(iv) Delivery/distribution channel risk

(c) Depending on the risk circumstances and how it evolves, the Group adjusts its risk assessment from time to time and reviews the extent of CDD, level of ongoing monitoring and risk mitigation measures to be applied to reasonably control money laundering risks.

(d) The Group keeps records and relevant documents of the risk assessment conducted.

4.4 Customer/counterparty Due Diligence ("CDD")

(a) The Group carries out CDD measures to identify and evaluate the potential risks before establishing business relationship or entering into transactions.

(b) The Group implements appropriate CDD measures according to its business activities for customer/counterparty identification and verification, ongoing monitoring (if applicable) and reporting of suspicious activity. The CDD measures should include at least the following steps:
   (i) obtaining the basic information of customer/counterparty ("CCD Information"), such as trade or business nature, identity and ownership structure;
   (ii) verifying the identity of customer/counterparty, and its beneficial owner(s) or controller(s) in case of non-natural person, by using reliable and independent sources of information, such as official documents and databases, or third-party verification services where necessary;
   (iii) if an agent purports to act on behalf of the customer/counterparty, identifying the agent and taking reasonable measures to verify the agent's identity and his/her authority to act on behalf of the customer/counterparty;
   (iv) requesting customer/counterparty to make update if there is any subsequent change to its CCD Information;
   (v) screening name of customer/counterparty against certain sanctions lists issued by but not limited to the UN and the competent authority in the jurisdictions in which the Group operates, if any customer/counterparty or its beneficial owner/controller/agent found to be locating, residing, domiciling, organised in any countries/regions listed thereon, reporting to the senior management.

(c) Employees must follow all due diligence procedures implemented to conduct assessment.

(d) Knowing your customer/counterparty procedures are not generally required for the customers of the supermarket business of the Group, the Government of PRC and HK and their respective departments, banks, and any company under the Group.

(e) The Group and its employees shall only proceed with transactions with customer/counterparty where it is satisfied that the transactions would not be in breach of the Policy and would not be involved in any money laundering activities.

4.5 Ongoing Monitoring

(a) Adopting a risk-based approach, appropriate ongoing monitoring of the business relationship and transactions with new and existing customer/counterparty is applied, where applicable. The measures may include:
   (i) from time to time review documents, data and information related to the customer/counterparty obtained for the purpose of CDD to ensure that they are up-to-date and relevant;
   (ii) conduct appropriate scrutiny of transactions to ensure that they are consistent with the Group's knowledge of the customer/counterparty and its business, risk profile and source of funds; and
   (iii) identify transactions that are complex, unusually large in amount or of an unusual pattern or that have no apparent economic or lawful purpose and which may indicate money laundering.

(b) The frequency of review and the extent of monitoring should be proportionate with the risk profile of the customer/counterparty through the risk assessment. Review should also be conducted when triggering events such as below occur:
   (i) a significant transaction (i.e. in terms of monetary value or where the transaction is unusual or not in line with the Group's knowledge of the customer/counterparty) is to take place;
   (ii) a material change occurs in the customer/counterparty's ownership;
   (iii) customer/counterparty documentation standards change substantially; or
   (iv) the Group is aware that it lacks sufficient information about the customer/counterparty concerned.

4.6 Suspicious Transactions Reporting

(a) When employees identify or suspect that a transaction is related to money laundering activity, they must report the case to their respective department heads who should evaluate to report to the senior management of the Group. If applicable, such suspicious transaction should be reported to the relevant authority of the government.

(b) In the event of a report being made to the relevant authority of the government, it is an offence if an employee discloses to the customer/counterparty and any other person any matter which is likely to prejudice any investigation which might be conducted following the disclosure (commonly referred to as "tipping-off"). Therefore, the employees concerned shall keep the relevant case strictly confidential.

4.7 Record Keeping

(a) The Group must maintain the original or a copy of all relevant records of customers/counterparties, transactions, etc. to meet the record-keeping requirements under the relevant regulatory requirements.

(b) All of the abovementioned records must be kept for at least 5 years from the end of the business relationship or the date of the transaction as applicable.

5. Review and Disclosure of this Policy

5.1 The board of the Company will continually review this Policy as appropriate from time to time. The latest version of this Policy is posted on the Group's website.