China Lesso Group Holdings Limited

(Incorporated in the Cayman Islands with limited liability)

(Stock code: 2128)

("the Company")

Information Security and Privacy Protection Policy ("this Policy")

1. Purpose

China Lesso Group Holdings Limited (hereinafter referred to as "the Company") attaches great importance to information security and privacy protection. The Company strictly complies with the *Cybersecurity Law of the People's Republic of China*, the *Data Security Law of the People's Republic of China*, the *Personal Information Protection Law of the People's Republic of China*, as well as any other applicable laws and regulations of relevant jurisdictions. The Company advances the development of its information security management system with reference to ISO/IEC 27001 and implements protective measures for information and data security. This Policy is hereby formulated to regulate information handling practices, ensure information security, and safeguard the legitimate rights and interests of relevant parties.

2. Scope of Application

This Policy applies to all personnel as well as all business and operational activities of the Company, its subsidiaries, branches, and holding enterprises, covering the entire information lifecycle from collection through storage, processing, transmission, and use to destruction. The Company requires any suppliers, distributors, partners, or any other stakeholders engaging in business with the Company to actively comply with this Policy and jointly build a secure and reliable information environment.

3. Responsible Department

The Information Management Center takes the main responsibility for information security and privacy protection. The Center is tasked with overseeing and coordinating efforts in this area, which include policy formulation, revision, implementation oversight, training, awareness campaigns, as well as the receipt, investigation, and handling of any privacy issues. The head of each department is the first responsible person for information security and privacy protection within their respective department, ensuring that all personnel in the department strictly comply with relevant regulations and work together to safeguard the information security of the Company's information system.

4. Content

4.1 Risk Management

The Company continuously works to improve and upgrade its information security management system, integrating the implementation of information security management policies and related tasks into its risk and compliance management processes. Based on regular identification, assessment, and analysis of information security and privacy protection risks, the Company develops and implements corresponding prevention and control measures and emergency plans to address them. The Information Management Center monitors and collects various types of information security threat intelligence through security threat intelligence platforms, industry security websites, and cooperation with third-party security agencies, and conducts evaluation and analysis on the collected threat intelligence. In case of any threats assessed as high-risk, internal response measures are promptly formulated, and early warnings are issued through the corporate email or internal systems to guide all departments in implementing necessary security precautions.

4.2 Information Security Management System

In accordance with the Plan-Do-Check-Act (PDCA) cycle, the Information Management Center has established and been operating an information security management system. Annually, the Internal Auditing Department takes the lead in conducting a systematic internal audit of the Company's information security management. The Company continuously improves its

information security management system by analyzing various security inspection results and staying abreast of industry security trends and the latest threat intelligence.

4.3 Internal and External Audits

The Internal Auditing Department conducts regular internal information security audits to verify the implementation of this Policy in all departments. In addition, qualified third-party institutions are regularly invited to conduct external audits, especially reviewing data compliance and privacy protection. Any issues identified in audits require rectification within a specified time frame, with rectification results incorporated into departmental performance evaluations to ensure the effective implementation of this Policy.

4.4 Information and Data Security

To ensure the confidentiality, integrity, and availability of information and data, the Company strengthens security controls throughout the information transmission lifecycle. Protective measures, including encryption technology deployment, access controls, data backup, and backup data recovery, are implemented to prevent information and data from being tampered with, leaked, or destroyed.

4.5 Employee Individual Responsibilities and Training

The Company clarifies the individual responsibilities of all employees in information security and privacy protection. Each employee is obligated to protect the Company's information assets and customer data, and strictly comply with security operating procedures. The Company conducts regular training to enhance employees' awareness of information security and confidentiality, ensuring that they understand and fulfill their role-specific information security responsibilities.

4.6 Security Incident and Vulnerability Reporting Process

The Company establishes and maintains clear and accessible reporting channels for security incidents, vulnerabilities, or suspicious activities, ensuring that all employees can promptly report potential security risks. When employees discover any information security incidents, system vulnerabilities, or suspicious activities involving information or privacy security, they should promptly report them to the Information Management Center. The Center will conduct an assessment and confirmation immediately after receiving the report, and initiate the corresponding response and handling procedures. Security threats can be effectively addressed by establishing and implementing the reporting process, minimizing security risks.

4.7 Privacy Information Collection and Usage Management

When collecting customers' personal information, the Company clearly informs them of the scope and purpose of collection and obtains their consent. Customers' personal information is stored within a reasonable and necessary period as stipulated by legal provisions, and various security measures aligned with industry standards to prevent its leakage. The Company actively establishes a data classification and grading system, data security management specifications, and data security development guidelines to manage and regulate the storage and use of personal information, ensuring that the collected personal information is relevant to the services provided by the Company.

4.8 Partner Management

The Company requires partners (including suppliers, etc.) to actively cooperate with relevant systems and requirements for information security and privacy protection. Before establishing cooperative relationships with key partners, the Company actively conducts information security-related due diligence to ensure that no major risks exist. Additionally, partners are required to sign confidentiality agreements to clarify mutual confidentiality responsibilities and obligations. The Company implements full-process information security management for suppliers, clarifying their security responsibilities and operational protocols for accessing information assets. Information protective measures, including authorization procedure standardization,, regular authorization appropriateness review, and dynamic authorization scope adjustment, aim to prevent leakage of sensitive information due to improper authorization and ensure the security and confidentiality of the Company's information assets.

4.9 Third-Party Disclosure Policy

When sharing, transferring, or providing relevant data to third parties, the Company commits to full compliance with relevant laws, regulations, and privacy protection guidelines of the nation, its place of incorporation, and its listing place to ensure that data transfer activities are lawful and respect the rights of data subjects. The purpose and scope of data transfer shall not exceed what was declared at the time of collection. Sensitive and confidential data must be transmitted through secure channels or in encrypted form. The data provider must obtain explicit commitments from the recipient. For cross-border data transmission, the requirements of local laws and regulations must be followed.

4.10 Business Continuity Management

In its business impact and risk analyses, which are centered on information security assurance needs, the Company identifies critical systems that support information security based on various factors, and conducts regular security risk assessments on the information system with practical analysis on the impact and likelihood of security risks. Annually, the Company conducts a comprehensive assessment and audit of emergency information security risk prevention measures and emergency response work, and incorporates information security assurance into the comprehensive risk management system to ensure the continuity, effectiveness, and compliance of information security management.

5. Supervision and Revision

This Policy shall be effectively implemented under the oversight of the Board of Directors. The Board of Directors hereby authorizes the Sustainable Development Committee to conduct daily monitoring and regular reviews, with the objective of ensuring the continuous suitability, adequacy, and effectiveness of this Policy in addressing any emerging cyber threats and meeting legal and regulatory requirements. In case of any significant changes in internal or external conditions, the Committee will promptly put forward a revision proposal to the Board of Directors, which shall be implemented upon approval by the Board of Directors.

6. Information Disclosure

The full text of this Policy, as well as key plans and actions related to information security and privacy protection, will be communicated to all personnel working for the Company through announcements, training, and other methods, and will be disclosed on the Company's official website for public access.

7. Supplementary Provisions

This Policy shall be interpreted by the Company's Board of Directors. It shall take effect upon approval by the Board of Directors, and so shall any amendment hereto.