REGULATION ON ENSURING TRANSPARENCY

I. GENERAL PROVISIONS

1. Abbreviated and defined terms:

Employees: Officers and employees.

Vingroup: Vingroup Joint Stock Company.

The Group: shall be construed as including Vingroup and Vingroup's subsidiaries as determined in accordance with applicable laws, accounting standards (as applied from time to time), and the Charter of Vingroup.

SMP: Senior management personnel.

Supplier: service providers, including agents, advisers, consultants, and contractors/ suppliers, acting on behalf of the Group.

2. Scope and Subjects of Application

2.1. This Regulation sets out measures to ensure transparency in the Group's production and business activities, including provisions on: (i) anti–money laundering; (ii) anti-bribery and anti-corruption; (iii) control of related-party transactions; and (iv) foreign law sanctions measures that must be known and complied with so as not to adversely affect the Group's operations.

2.2. This Regulation applies to all officers and employees (including probationary employees and apprentices/trainees) assigned to perform tasks related to the matters governed by this Regulation, and may also be required to apply to Suppliers and Related Persons, in accordance with the detailed provisions of this Regulation.

II. REGULATIONS ON ANTI–MONEY LAUNDERING

When the Group conducts business in sectors exposed to money-laundering risks and is required to make reports in accordance with the Law on Anti–Money Laundering, it must apply anti–money laundering measures in compliance with the applicable anti–money laundering laws and this Regulation.

1. Customer Due Diligence/Customer Identification

1.1 The department directly dealing with Customers shall be responsible for conducting face-to-face meetings to collect and verify Customer/Beneficial Owner identification information. For transactions using technology that allows Customers to perform transactions without face-to-face interaction with the Group's personnel, direct meetings with Customers may not be required; however, appropriate measures, methods and technologies must be in place to identify and verify Customers with all information required under these Regulations.

1.2 **Customer identification information:**

1.2.1 For individual customers:

a. Individual customers of Vietnamese nationality: full name; date of birth; nationality; occupation and position; contact phone number; identity card number or citizen identification number or personal identification number or passport number, date of issue and place of issue; registered address of permanent residence and current residence (if different);

b. Individual customers of foreign nationality residing in Vietnam: full name; date of birth; nationality; occupation and position; contact phone number; passport number, date of issue and place of issue; entry visa number, except where visa exemption applies in accordance

with applicable laws; registered address of residence in the foreign country and registered address of residence in Vietnam;

c. Individual customers of foreign nationality not residing in Vietnam: full name; date of birth; nationality; occupation and position; passport number or other identification information issued by a competent foreign authority, date of issue and place of issue; registered address of residence in the foreign country;

d. Individual customers holding two or more nationalities: the relevant information as prescribed in items (a), (b) or (c) above; nationality and registered address of residence in the country of the other nationality(ies);

e. Stateless individual customers: full name; date of birth; occupation and position; international travel document number (if any), visa number; visa-issuing authority, except where visa exemption applies in accordance with applicable laws; registered address of residence in the foreign country (if any) and registered address of residence in Vietnam.

1.2.2 For institutional customers: full trading name and abbreviated name (if any); address of the head office; establishment license number, enterprise registration number or tax code; contact phone number; fax number and website (if any); lines of business and business operations; information on the founders, legal representatives, Director or General Director, Chief Accountant or person in charge of accounting (if any) of the institution, including the corresponding information prescribed in Section 1.2.1 of Part II and the information prescribed in this Section 1.2.2 of Part II in cases where the founder is an organization.

1.3 Beneficial owner information shall include individual customer identification information as prescribed in Section 1.2.1 of Part II and/or as required by applicable laws from time to time.

1.4 Updating Customer identification information: Business units shall continuously update Customer identification information throughout the duration of the business relationship with the Customer; and ensure that transactions conducted by the Customer through such units are consistent with the information known about the Customer, the Customer's business activities, money-laundering risk level, and the source of the Customer's assets.

1.5 Verification of Customer Identification Information:

1.5.1 Business units shall use documents and data to verify Customer identification information, including:

a. For individual customers: valid identity card, citizen identification card or passport; and other documents issued by a competent authority.

b. For institutional customers: establishment license, decision on establishment or enterprise registration certificate; decisions on reorganization, dissolution, bankruptcy or termination of operations of the institution (if any); the institution's charter; decisions on appointment or employment contracts of the Director or General Director, Chief Accountant or person in charge of accounting (if any); and documents and data relating to the founders, legal representatives of the institution and beneficial owners.

1.5.2 Business units may use third parties to identify and verify Customers through the following methods:

a. Through a third party being a financial institution or a designated non-financial business or profession that has established a relationship with the Customer, excluding agency and outsourcing relationships. Such institution must be subject to the management and supervision of a competent authority and must maintain confidentiality in accordance with applicable laws;

b. Through regulatory authorities or other competent State authorities to collect information and cross-check it against the information provided by the Customer;

c. Engaging other organizations that have the appropriate functions and satisfy conditions prescribed by law to verify Customer identification information.

2. Categorization and handling of Customers by risk level

2.1 Customers shall be categorized by risk level based on the following criteria:

2.1.1 By type of Customer: resident or non-resident; institutional or individual Customers; Customers included or not included in (i) the Blacklist (including lists of organizations and individuals related to terrorism and terrorism financing compiled under the leadership of the Ministry of Public Security, and lists of organizations and individuals designated as related to the proliferation and financing of proliferation of weapons of mass destruction compiled under the leadership of the Ministry of National Defence in accordance with applicable laws); (ii) the Warning List (lists of organizations and individuals compiled by the State Bank of Vietnam to warn of organizations and individuals with a high risk of money laundering); and (iii) the list of organizations and individuals requested or prohibited from being provided with services or products compiled by the Anti-Money Laundering Department under the Banking Supervision Agency of the State Bank of Vietnam and other relevant State authorities; as well as the Customer's business sectors, methods and operations.

2.1.2 By type of products or services used or expected to be used by the Customer: cash or wire transfer services; payment or money transfer services; money exchange services; brokerage, trust or authorization services.

2.1.3 By geographical location where the Customer resides or has its head office: countries subject to sanctions under resolutions of the United Nations Security Council; countries publicly listed as non-compliant or partially compliant with recommendations on anti-money laundering and combating the financing of terrorism issued periodically by the Financial Action Task Force; countries, regions or territories assessed as having high levels of drug trafficking, corruption or money laundering activities.

2.1.4 Other factors (if any).

2.2 Risk-based Customer Handling Measures:

2.2.1 Low-risk Customers: The Group may apply simplified customer due diligence measures after the initial establishment of the business relationship, including one or all of the following:

a. Not collecting information on the purpose and intended nature of the business relationship where such purpose and nature can be inferred from the types of transactions or business relationships already conducted or established;

b. Verifying the identity of the Customer and the Beneficial Owner after the establishment of the business relationship;

c. Reducing the frequency of Customer identification updates;

d. Reducing the level of transaction monitoring and control.

2.2.2 Medium-risk Customers: Full customer due diligence measures as prescribed in Part II of these Regulations shall be applied.

2.2.3 High-risk Customers: Enhanced measures shall be applied as follows:

a. Obtaining additional information, including:

For individual Customers:

(i) The Customer's average monthly income for at least the most recent three (3) months;

(ii) The name, address and contact phone number of the agency, organization or business owner where the Customer works or from which the Customer derives his or her primary income.

For institutional Customers:

(i) The business lines, production, trading or service activities generating the primary revenue;

(ii) Total revenue for the most recent two (2) years;

(iii) A list (full names and permanent addresses) of members of the Board of Directors or Members' Council, members of the executive management, the Chief Accountant or equivalent positions;

(iv) The name, address and legal representative or authorized representative of the parent company (if the Customer is a subsidiary), or a list of names, addresses and legal representatives or authorized representatives of branches, subsidiaries and representative offices (if the Customer is a parent company).

b. Monitoring Customer transactions to ensure that such transactions are consistent with the nature and purpose of the established relationship and the Customer's business activities; promptly detecting unusual transactions and reviewing and reporting suspicious transactions where there are reasonable grounds in accordance with applicable laws.

c. Periodic information updates at least once every one (1) year or upon becoming aware of any change in Customer information.

2.2.4 Procedures and task delegation:

a. On a daily basis, the department directly dealing with or receiving Customers, through technological measures, shall prepare a list and information of Customers requesting or accepted to establish transactions with the Group and submit such list to the department responsible for reviewing, detecting, handling and reporting suspicious transactions (the "**Suspicious Transaction Control Unit**"); or report any unusual signs to the Suspicious Transaction Control Unit for review and handling in accordance with regulations.

b. The Suspicious Transaction Control Unit shall review Customer information and cross-check such information against the Blacklist, Warning List, lists of organizations and individuals requested or prohibited from being provided with services or products received by the Group from competent State authorities, and the list of large-value transactions (being transactions in cash, gold or foreign currency in cash with an aggregate value equal to or exceeding the threshold prescribed by competent State authorities, conducted once or multiple times in a day), in order to detect suspicious transactions (being any transaction showing unusual signs or having reasonable grounds to suspect that the assets involved are derived from criminal activities or related to money laundering). The Unit shall propose that the designated professional officer decide on appropriate measures to be applied prior to establishing the transaction with the Customer and notify the department directly dealing with the Customer for coordination and implementation.

c. For Customers classified as high-risk in accordance with the Law on Anti–Money Laundering and the Group's Customer categorization regulations, the Suspicious Transaction Control Unit shall be responsible for applying the enhanced measures prescribed in Section 2.2.3 of Part II.

3. Review, Detection and Handling of Suspicious Transactions

3.1 Review and detection of suspicious transactions

3.1.1 All officers and employees assigned to perform tasks related to transactions subject to anti–money laundering measures shall carefully review records, documents and information relating to the transactions and the relevant Customers in order to promptly detect transactions showing suspicious signs; apply the measures prescribed in these Regulations and/or propose and report to their direct supervisors and the Group's designated professional officer for review and approval of the application of anti–money laundering measures in accordance with these Regulations.

3.1.2 The Suspicious Transaction Control Unit shall regularly review and update Customer identification information throughout the period during which the Customer establishes transactions with the Group; apply professional anti–money laundering measures as prescribed to detect, propose handling measures and report suspicious transactions and large-value transactions in accordance with regulations to the Group's designated professional officer for review and approval.

3.1.3 The Group's designated professional officer shall be responsible for regularly inspecting and supervising the application of anti–money laundering measures within the Group; approving documents and reports of the Group to be submitted to competent State authorities in relation to anti–money laundering; organizing the storage and retention of Customer identification information, relevant documents and reports in accordance with the Law on Anti–Money Laundering and the Group's internal regulations; assessing the Group's compliance with anti–money laundering regulations; and organizing training on anti–money laundering operations and other provisions in this Part.

3.2 Application of temporary measures:

3.2.1 Transaction-delay measures shall be applied in the following cases:

a. Where there are grounds to suspect or detect that parties related to the transaction are included in the Blacklist;

b. Where there are reasonable grounds to believe that the requested transaction is related to criminal activities, including transactions requested by a person convicted under criminal procedural laws where the assets involved are owned by or originate from the ownership or control of such convicted person; or transactions related to organizations or individuals involved in terrorist financing crimes;

c. Where required by competent State authorities in accordance with relevant laws.

3.2.2 Upon applying transaction-delay measures, the reporting entity shall immediately report to competent State authorities and the State Bank of Vietnam.

3.2.3 The duration for applying transaction-delay measures shall not exceed three (3) working days from the date of commencement. If, upon the expiry of such period, the Group does not receive any response from the competent State authorities specified in Section 3.2.2 of Part II, the Group may proceed with the transaction.

3.2.4 The Group shall comply with decisions of competent State authorities regarding the freezing of accounts, sealing, freezing or temporary seizure of assets of organizations or individuals in accordance with applicable laws.

3.2.5 The application of temporary measures must ensure the principle that it does not adversely affect the Group's and Customers' general business operations, while remaining compliant with applicable laws.

3.2.6 Temporary measures must be applied to the appropriate subjects and circumstances and shall be reported to the Group's designated professional officer for timely decision-making.

3.3 Suspicious transaction reports, large-value transaction reports, control reports and internal audit reports on anti–money laundering shall be prepared and submitted in accordance with applicable laws.

4. Record Retention, Information Confidentiality, and Internal Control / Internal Audit

4.1 The Group shall retain the following information, documents, records and reports:

a. Customer identification information, files and documents;

b. Results of the Group's analysis and assessment of Customers and reportable transactions;

c. Other information, files and documents related to Customers and reportable transactions;

d. Reports on large-value transactions, suspicious transaction reports and electronic funds transfer transaction reports exceeding the value threshold prescribed by the Governor of the State Bank of Vietnam, together with accompanying information, files and documents.

4.2 Retention periods shall be as follows:

a. Five (5) years from the date of completion of the transaction, account closure or reporting date, for the information, files and documents specified in items (a), (b) and (c) of Section 4.1 of Part II;

b. Five (5) years from the date the transaction arises, for the reports specified in item (d) of Section 4.1 of Part II.

4.3 Customer information and documents are classified as confidential information and: (i) shall be provided to competent State authorities only upon approval by duly authorized SMP of the Group; and (ii) must not be disclosed the Customer or any related parties that a suspicious transaction report has been filed, nor the contents of such report, nor any information provided to competent authorities.

4.4 Annually, the Group shall conduct internal control and internal audits on anti–money laundering practices. Such internal control and audits may be conducted independently or in combination with other matters. All violations detected during internal control and audit processes shall be reported to the Group's designated professional officer for handling in accordance with the Group's internal regulations and may be reported to competent State authorities for handling in accordance with applicable laws.

III. ANTI-BRIBERY AND ANTI-CORRUPTION REGULATIONS

1. All officers and employees must comply with the Law on Anti-Corruption and the Group's anti-bribery and anti-corruption regulations.

2. Vingroup shall appoint the Head of the Inspection Division or another person to act as the compliance officer; each Vingroup subsidiary shall also appoint an employee to act as the compliance officer of such subsidiary (collectively, the "**Compliance Officer**") who shall be responsible for the implementation of this Policy, including but not limited to:

2.1 Receiving information on any actual or suspected acts of bribery or corruption within the Group or committed by any Supplier.

2.2 Any director, officer or employee of the Group, as well as any Supplier, who violates the anti-bribery and anti-corruption regulations (including acts of retaliation against whistleblowers; failure to cooperate in anti-bribery and anti-corruption activities as requested by the Group) shall be subject to internal disciplinary measures, contractual penalties and be reported to competent investigative authorities for handling in accordance with applicable laws.

3. Prohibited acts applicable to Suppliers:

3.1 Suppliers are prohibited from engaging in any of the following acts:

3.1.1 Suggesting, proposing or giving Gifts (Vietnamese currency, freely convertible foreign currency, valuable papers, goods, assets, services, rights of use, rights of enjoyment and other benefits convertible into money or other interests) to Government Officials in cases where the Group is involved in public service activities under the responsibility of such Government Officials, before, during or after the receipt of such Gifts;

3.1.2 Suggesting, proposing or giving Gifts to Government Officials who have influence over the business interests of the Group or any Supplier;

3.1.3 Suggesting, proposing or giving Gifts to Government Officials for the purpose of committing corrupt acts as stipulated under the Vietnamese Law on Anti-Corruption and/or for unclear or improper purposes;

3.1.4 Suggesting, proposing or giving money, assets or any other material benefits in any form to Government Officials in order for such officials to perform or refrain from performing an act at the request of the Group for the benefit of the Group.

3.2 The provisions in Clause 3.1.1 of Part III shall not apply to:

3.2.1 Travel expenses and related business expenses of Government Officials incurred for work-related purposes (for the performance or execution of a contract with the Government or for promoting the Group's services); or travel and related business expenses pre-approved by the Compliance Officer prior to payment; or expenses not pre-approved by the Compliance Officer but which do not violate Vietnamese law, are of insignificant value, consistent with customary practices, paid directly to service providers and fully and accurately recorded in the Group's books and records.

Where Suppliers bear travel expenses for Government Officials: invitations/advance notices must be sent to the relevant government authority rather than to a specific Government Official. Such invitations/advance notices must clearly state the business purpose and must not create any misunderstanding that such business practices constitute a concealed gift or benefit to any Government Official.

3.2.2 Meal and entertainment expenses including meal costs or entrance fees, hospitality at entertainment venues, sports venues, cultural events or mixed events may be accepted by the Group where they are unrelated to public duties assigned to such Government Officials before, during and after the receipt of such entertainment expenses, or where the Group is not subject to the management or control of such Government Officials; and only where such expenses do not violate applicable laws, are consistent with customary practices, are of insignificant value, serve legitimate business purposes and are fully and accurately recorded in the Group's books and records.

4. Requirements applicable to third parties in business activities:

4.1 Any payments made, promised, offered or authorized by third parties – agents, advisors, consultants, contractors or service providers – to any Government Official on behalf of the Group may give rise to liability under anti-corruption laws, and the Group shall conduct appropriate due diligence on the background and reputation of such third parties to ensure that such third parties act in compliance with the Group's requirements.

4.2 Any contracts with agents, advisors, consultants, contractors or service providers must comply with this Policy and include an anti-bribery undertaking clause in accordance with the Group's template attached to this Policy and as amended from time to time.

5. Political parties and candidate contributions

Any contributions, whether in cash or in kind, or any form of services provided by the Group to political parties or political candidates are prohibited under this Policy.

6. Charitable contributions

6.1 All charitable contributions must be lawful and for legitimate charitable purposes, and must be assessed and investigated for any potential red flags, including but not limited to the following:

6.1.1 Contribution amounts exceeding VND 500,000;

6.1.2 Contribution amounts or intended recipients proposed by a Government Official;

6.1.3 An employee, director or worker of the recipient organization being a Government Official or having a family relationship or close relationship with a Government Official;

6.1.4 Indications that the contribution may influence government actions or persuade the Government or a Government Official to provide business benefits to the Group;

6.1.5 The recipient organization requests contributions in cash;

6.1.6 The recipient organization does not issue a receipt for the contribution;

6.1.7 The recipient organization proposes anonymous contributions; or

6.1.8 The recipient organization requests contributions to be made in foreign currency or transferred directly to accounts in a third country.

6.2 Where any of the above red flags exist, the Compliance Officer must be consulted prior to making the contribution.

7. Training, implementation and audit

7.1 Group Employees shall be trained on anti-corruption matters and bribery and corruption control procedures.

7.2 The Compliance Officer is responsible for monitoring and ensuring Suppliers' compliance with this Policy and ensuring that this Policy remains consistent with changes in applicable laws.

8. Accounting and record keeping:

8.1 The Group is responsible for maintaining and reporting financial information to shareholders, government authorities and other stakeholders; maintaining accurate, complete and reasonably detailed accounting records to clearly reflect transactions and movements of the Group's assets.

8.2 Group Employees are prohibited from engaging in fraudulent accounting practices, including but not limited to theft, fraud, falsification of documents, evidence or records, or erasing, destroying or interfering with any accounting records of the Group or Customers, affiliated companies or agents of the Group.

8.3 Accounting records shall be prepared and retained in accordance with this Policy and the Group's document retention policies.

9. Procedures applicable to Government tenders

9.1 All bidding or tender documents for land development projects and/or Government projects ("**Tender Documents**") prepared by Suppliers for submission to the Government must be provided to the Compliance Officer in advance for review to ensure the following requirements are satisfied:

9.1.1 Tender Documents must be approved by the Compliance Officer prior to submission;

9.1.2 Tender Documents must fully comply with this Policy;

9.1.3 Suppliers must not collude with any individual or organization to submit Tender Documents for improper purposes;

9.1.4 Suppliers must refuse any proposal/offer to "secure the winning bid" related to the Tender Documents if there is reason to believe that a Government Official involved in the evaluation of the Tender Documents, or a Supplier (including any personnel, representatives, consultants, subcontractors or employees of such Supplier) involved in the submission of the Tender Documents, is directly or indirectly involved in corrupt, fraudulent, coercive, collusive, obstructive, or other prohibited practices in relation to the Tender Documents.

9.2 All records evidencing any amendments to the Tender Documents shall be retained for audit purposes in accordance with applicable regulations.

IV. INTERNAL TRANSACTION CONTROL REGULATIONS

1. Regulations on Insiders, Related Persons, Inside Information and Insider Trading

1.1 Insider(s): person who directly or indirectly knows, is shared with or has access to Inside Information, including but not limited to (i) employees; (ii) members of the Board of Directors and managers of the Group as prescribed under the Law on Enterprises.

1.2 Related Person(s): persons who has any relationship with an Insider and (i) is disclosed Inside Information by such Insider or (ii) has economic interest connections with such Insider.

1.3 Inside Information: any information relating to the Group that has not been publicly disclosed and which, if disclosed, may have a significant impact on the Group's securities price, existing in any form such as correspondence, printed or handwritten documents, faxes, emails, information storage

devices such as computer hard drives or external storage devices, exchanges, verbal communications or any other form that may be communicated to other parties.

1.4 Insider Transaction(s): transactions conducted by Insiders or Related Persons based on Inside Information.

2. Responsibilities of Insider:

2.1 To safeguard and strictly maintain the confidentiality of Inside Information and to use Inside Information solely for work purposes in accordance with this Regulation, relevant regulations of the Group/Company and applicable laws.

2.2 Not to conduct any Insider Transactions and to require Related Person(s) not to conduct any Insider Trading, except for the following transactions, provided that they are carried out cautiously and transparently, and must be reported to the relevant senior management of the Group upon request, and the Insider must independently consider and ensure that such transactions comply with applicable laws and other internal regulations of the Group:

2.2.1 Exercise of options under the ESOP (if the person conducting the transaction is an ESOP beneficiary), provided that all restrictions set out in the ESOP agreements and related documents are complied with;

2.2.2 Gifting, donation, inheritance or receipt by way of gift, donation or inheritance;

2.2.3 Change in the form of securities ownership without changing the owner, ownership rights or value of the securities (such as stock split, exchange of securities certificates, reissuance of securities certificates);

2.2.4 Transactions conducted after the Inside Information has been publicly disclosed through mass media in accordance with applicable laws;

2.2.5 Transactions permitted with the approval of competent senior management or pursuant to the Group's policies from time to time. In such cases, Insider Trading shall be conducted in accordance with the instructions and conditions approved and guided by the Group.

2.3 To the extent possible and within the scope of permitted responsibilities, to notify and require partners and relevant persons to be aware of and comply with the provisions of this Regulation. In cases where confidentiality agreements or equivalent documents are entered into, the relevant Insider shall be responsible for ensuring that such confidentiality agreements reflect the fundamental spirit of this Regulation.

V. NOTES ON FOREIGN SANCTIONS LAWS

1. Compliance obligations

1.1 The Group shall ensure that its business activities and transactions do not breach any obligations under any loan, credit, guarantee or other contracts or agreements to which the Group is a party, relating to sanctions measures or any Sanctions Laws ("**Sanctions Compliance Obligations**").

Sanctions Laws mean (i) any laws, regulations, executive orders or restrictive measures relating to trade, economic or financial matters administered, enacted, issued or enforced by the U.S. Department of the Treasury's Office of Foreign Assets Control ("**OFAC**"), the U.S. Department of State or any other U.S. governmental authority; and (ii) any laws, regulations or restrictive measures relating to trade, economic or financial matters administered, enacted, issued or enforced by the United Nations Security Council, the EU or any of its member states, Vietnam, Switzerland, Singapore or any other country or international organization.

1.2 The Group must ensure that none of its officers, employees, consultants or contractors are recruited or appointed as a Sanctioned Person.

A Sanctioned Person means any individual or organization that:

a. resides in, is established under the laws of, or is owned or controlled by, or acts on behalf of a person residing in or established under the laws of any country or territory that is subject to comprehensive sanctions under applicable Sanctions Laws;

b. is designated, or owned or controlled by a designated person, or acts on behalf of a designated person on the "Specially Designated Nationals and Blocked Persons" list of OFAC, or any similar list (including any list of specially designated sanctioned individuals or entities) issued by, or any announcement regarding the imposition of Sanctions Laws made by, the U.S. Department of State, the U.S. Department of Commerce, the U.S. Department of the Treasury or any other U.S. governmental authority, the United Nations, the EU, Vietnam, the Monetary Authority of Singapore or the Swiss State Secretariat for Economic Affairs; or

c. is subject to transaction prohibitions under any applicable Sanctions Laws.

1.3 The Group ensures that it does not conduct business or engage in transactions, whether directly or indirectly, with any Sanctioned Person in a manner that may result in a breach of any Sanctions Compliance Obligations or any applicable Sanctions Laws. In addition, the Group must ensure that its officers, employees, consultants and contractors do not conduct any business activities (on behalf of and in the name of the Group) with any Sanctioned Person in a manner that may result in a breach of any Sanctions Compliance Obligations or any applicable Sanctions Laws to the Group.

1.4 The Group shall not, directly or indirectly, use or permit the use of any funds sourced from, or received by, or contributed to, or facilitate the use of any funds by any individual or entity (whether related to the Group or not) to finance the activities of any Sanctioned Person, in any manner that may result in a breach of any Sanctions Compliance Obligations or any Sanctions Laws applicable to the Group..

1.5 The Group shall not use any revenue or payments derived directly or indirectly from transactions prohibited under any applicable Sanctions Laws.

1.6 The Group does not conduct business in any Sanctioned Territory (or with any individual or organization residing or established therein) in a manner that may result in a breach of any Sanctions Compliance Obligations or any applicable Sanctions Laws to the Group. In addition, the Group ensures that its officers, employees, consultants and contractors do not conduct business (on behalf of the Group) with any individual or organization residing or established in a Sanctioned Territory, or take any other actions in a manner that may result in a breach of any Sanctions Compliance Obligations or any applicable Sanctions Laws to the Group.

Sanctioned Territory means any country or territory that is subject to sanctions under any applicable Sanctions Laws.

1.7 All contracts entered into with the Group by Customers, consultants, contractors, service providers, suppliers, or other partners must include an undertaking that neither they nor any of their managers, employees, or representatives (i) are in breach of, or are subject to, any proceedings, litigation, claims, or investigations relating to any Sanctions Laws; or (ii) are a Sanctioned Person.

2. Compliance Officer

2.1 The Compliance Officer is responsible for overall monitoring of the implementation of this Regulation throughout the Group.

2.2 The Compliance Officer is responsible for regularly updating the Board of Directors on compliance with Sanctions Compliance Obligations and Sanctions Laws.

3. Handling non-compliance

3.1 Any officer or employee of the Group, upon becoming aware of any violation or potential violation of any Sanctions Compliance Obligations or any applicable Sanctions Laws to the Group, must immediately report such matter to the relevant Compliance Officer for timely and appropriate handling.

3.2 In the event that any contract entered into by the Group and currently in effect, due to (a) changes in Sanctions Laws; or (b) a change-of-control event affecting the counterparty to such contract, results in continued performance of the contract violating Sanctions Compliance Obligations or Sanctions Laws, the department responsible for monitoring the performance of such contract must immediately notify the Compliance Officer.

The Compliance Officer is responsible for reviewing the contract and the specific circumstances to provide advice on appropriate handling measures. In complex cases, the Compliance Officer must seek instructions from the responsible management. Based on management's instructions and the Compliance Officer's recommendations, relevant departments and units shall take all necessary actions to address the violation, including but not limited to amendment, suspension, cancellation and/or termination of the contract.

3.3 Any officer, employee, consultant or contractor who violates this Regulation shall be subject to disciplinary measures, which may include suspension, termination of employment and/or termination of any related contracts in accordance with applicable laws.

TEMPLATE OF CLAUSE ON ANTI-CORRUPTION AND ANTI-BRIBERY

ARTICLE [ ][1]: ANTI-BRIBERY UNDERTAKING

1. Party A[2] represents, warrants and undertakes that its managers, employees, agents, or any person (hereinafter referred as "**Party A's Personnel**") whether directly or indirectly contacting, dealing or working with Party B[3], shall (i) not offer, promise, give or authorize the giving of any bribe, including any gift, kickback, commission, payment, asset (cash or in kind), or thing of value/other benefit (generally called a "**Bribe**"), to any manager, employee or any person of Party B (hereinafter referred as "**Party B's Personnel**") and/or (ii) not through any third party to offer or give a Bribe to Party B's Personnel in order to obtain preferential treatment in the award/entering into of any contract/agreement with Party B or to secure any waiver of any obligations under such contract/agreement, and/or to obtain any other non-transparent, unfair or improper advantage.

   For the avoidance of doubt, a Bribe includes any act occurring before, during or after the performance of the Contract/Agreement with Party B.

   Where Party A and/or any Party A Personnel becomes aware that any Party B Personnel requests, solicits or demands a Bribe, Party A shall promptly notify/report to Party B via:

   Hotline: 0988428787 Email: gopy@vingroup.net

2. If Party A violates this Article, Party B may, at any time, apply one or all of the following measures:

(i) To cancel the tender/bidding award decision (or selection result) where Party A was selected through a tender/bidding process; and/or disqualify/debar Party A from participating in other tenders/bidding packages of Party B; and / or

(ii) To revoke/withdraw any approvals, consents, permissions or benefits obtained by Party A, or any approvals/acceptances granted by Party B in connection with the negotiation, execution and/or performance of the Contract/Agreement that are tainted by the Bribe; and / or

(iii) Depending on the severity of the bribery act, impose a contractual penalty[4] of VND 150,000,000 (one hundred and fifty million Vietnamese Dong) per violation and/or terminate the Contract/Agreement immediately without any liability to Party A. In addition, Party A shall indemnify Party B for all losses and damages (if any) arising from such termination, refund to Party B any advance/prepaid amounts already paid to Party A, and be subject to other remedies/penalties under the Contract/Agreement as applicable to termination due to Party A's breach; and / or

(iv) To refer the matter and relevant documents to competent authorities for investigation and handling in accordance with applicable criminal laws.

3. Party A shall indemnify, defend and hold harmless Party B from and against any and all losses, damages, liabilities, claims, penalties, fines, costs and expenses (including reasonable attorneys' fees and administrative costs) arising out of or in connection with any bribery act by Party A or any Party A Personnel.

---

[1] To be numbered correspondingly in the contract/agreement.
[2] Party A is a counter-party, or a goods/service supplier.
[3] Party B is Vingroup or a subsidiary of Vingroup.
[4] A penalty of VND 150,000,000 shall apply, except for contracts with a value below VND 500,000,000, for which the Parties may agree in the Contract on a penalty ranging from 10% to 15% of the contract value per breach.