GIVEX INFORMATION TECHNOLOGY GROUP LIMITED

POLICY RELATING TO ANTI-MONEY LAUNDERING AND ANTI-TERRORIST FINANCING

(Adopted and approved by the Board on November 30, 2021)

A. INTRODUCTION

"**Money laundering**" consists of any act or attempted act to channel (in almost any manner or any means, including by sending, delivering, transferring, altering, disposing, using, etc.) into legitimate financial and economic circulation currency or monetary instruments, or any property or proceeds originating from criminal activities such as bribery, drug-trafficking and terrorism, with intent to conceal or convert the property or proceeds.

"**Terrorist financing**" is the act of channeling currency or monetary instruments, or providing or collecting property, for the purposes of undertaking or facilitating terrorist activities such as intentionally causing death or serious bodily harm or endangering an individual's life, or causing substantial damage to a property that is likely to kill, seriously harm or endanger an individual.

Money laundering and terrorist financing are both criminal offences. Givex Information Technology Group Limited and its subsidiaries, if any (collectively, the "**Company**"), are committed to deterring and detecting money laundering and terrorist financing and in no way does the Company condone, facilitate or support such activities. To this end, this Policy Relating to Anti-Money Laundering and Anti-Terrorist Financing (the "**Policy**") re-affirms the Company's commitment, as expressed in the Code of Business Conduct and Ethics of the Company, as may be amended and updated from time to time (the "**Code**"), to comply with all the laws, rules and regulations, including those designed to combat money laundering and terrorist financing.

B. APPLICATION

This Policy applies to all directors, officers and employees of the Company and its subsidiaries.

C. OVERVIEW

This Policy is created to assist directors, officers and employees of the Company and its subsidiaries in conducting the dealings of the Company appropriately such that legitimate business activities are distinguished from illegal or suspicious activities which are connected in whole or in part with money laundering and terrorist financing. To this end, this Policy should be considered to form an integral part of the Code with which all directors, officers and employees of the Company are required to comply.

In general, anyone subject to this Policy and the Code should:

- not knowingly instigate or otherwise participate in any money laundering or terrorist financing schemes;
- conduct appropriate risk-based review and due diligence of all third parties dealing with the Company;
- not deal (directly or indirectly) with persons known to be involved in such schemes; and
- report any illegal, suspicious or abnormal activity immediately.

Those subject to this Policy and the Code will be expected to rely on their professional judgment to determine what is reasonable and what is suspicious or abnormal in normal business circumstances. In particular, you should be wary of "red flags" such as:

- Payment irregularities including:
    - payments made by someone not party to a contract;
    - payments to or from accounts other than normal business relationship accounts;
    - requests to make multiple payments for one invoice for no apparent reason;
    - requests for overpayment;
    - attempts to make payments for cash equivalents; and
    - request to make payments in countries different from the place of business of contractual party, or that are tax safe havens.

- Contracting irregularities including:
    - "secret contracts" or contracts that cannot be known or approved by the persons normally in charge of the processes;
    - contracts executed with parties that have not been good performers in previous contracting experiences; and
    - parties that fail to provide all information, provide inconsistent or incomplete information, or that are reluctant to explain when asked.

- Contractual parties who appear to lack integrity, which requires:
    - continual assessment of the integrity of current and potential business relationships in addition to compliance with any business relationship identification requirements of the Company; and
    - regular communication with current and potential business relationships as to the Company's expectations under the Code and this Policy.

An integral part of this Policy is compliance with the sections of the Code entitled "Accuracy of Books and Records", and "Accounting, Auditing or Disclosure Concerns", which will provide the Company with an opportunity to monitor transactions above and beyond the exercise of professional judgment of employees closely involved in any business relationship and transaction.

As an employee, if you believe that a violation of this Policy or the Code has occurred, or if you suspect any illegal, suspicious or abnormal activity that may be related to money laundering or terrorist financing, you have an obligation to promptly report the relevant information to your supervisor. However, if you feel uncomfortable approaching your supervisor, or if you have any specific or general questions, you may contact, the Chair of the Audit Committee or the Chief Financial Officer. Directors and officers should promptly report any violations or suspicions to the Chair of the Board of Directors or to the relevant committee Chair.

Sections of the Code entitled “Treatment of Reports and Complaints”, “Penalties for Violation of the Code”, “Disciplinary Action for Code Violations”, and “Legal Notice” apply equally to this Policy, as if references to the Code in the foregoing referenced sections were replaced with references to this Policy.

The consequences of non-compliance with the applicable laws, rules and regulations regarding money laundering and terrorist financing, and with this Policy, are not only significant criminal, civil and disciplinary penalties but also considerable reputational harm from any association with such activities.