AML Policy

1. Purpose of this Know Your Client / Anti-Money Laundering Policy

1.1. In this know your client ("KYC") / anti-money laundering ("AML") policy (the "Policy"), we, SMX Operations Limited (the "Company"), set out the principles and procedures for:

- identifying and verifying the identity of our customers (the term "customers" covers both clients (i.e. business) and contractors of the Company registered or registering on the platform located at: https://www.sendico.io/ (the "Platform")); and
- preventing and actively deterring money laundering, terrorist financing and any other criminal abuse of the Company's Services.

This Policy applies to all users and customers who wish to purchase the Company's services (the "Services"), which are provided under the terms of service and other applicable documents located at https://www.sendico.io/ , including its subdomains, regardless of the form of payment.

1.2. For the purposes of implementing this Policy, the Company may engage one or more external KYC/AML service providers (each a "KYC/AML Service Provider", together the "KYC/AML Service Providers").

1.3. This Policy is designed to ensure that the Company complies, to the extent applicable to its activities, with the anti-money laundering and counter-terrorist financing regime of Hong Kong Special Administrative Region, including in particular:

- the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615);
- the Organized and Serious Crimes Ordinance (Cap. 455);
- the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405);
- the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575); and
- any subsidiary legislation, guidelines, codes, circulars and directions issued by the relevant Hong Kong authorities that are applicable to the Company's business model (collectively, the "Hong Kong AML/CTF Laws").

1.4. This Policy, and any procedures adopted under it, shall be governed by and construed in accordance with the laws of Hong Kong SAR, without prejudice to the mandatory provisions of other jurisdictions that may also apply to the Company's activities.

2. Customer due diligence and "know your client" identification program

2.1. The Company, or a person designated by the Company (including any KYC/AML Service Provider), will collect information and documents from each customer who has created a user account on the Platform, in order to identify that customer and assess

relevant risks in accordance with this Policy and the Hong Kong AML/CTF Laws. The Company follows, at minimum, the following principles:

- applying a risk-based approach to identify and verify each customer;
- recording and retaining all information and documents obtained from the customer;
- notifying customers that the Company will request identification information to verify their identity;
- checking whether a customer (or related person) appears on relevant international and national sanctions, terrorism, and other watchlists, including those recognised or required under Hong Kong AML/CTF Laws.

2.2. The Company will apply enhanced due diligence and additional verification measures, or refuse to establish or maintain a business relationship, in particular where:

- the customer (or related person) is from, or associated with, a high-risk jurisdiction identified by the Company or competent authorities;
- the business relationship or transaction exhibits features of heightened ML/TF risk (e.g., complex, unusually large, lacking clear economic rationale);
- the customer is a politically exposed person (PEP), or a family member or close associate of a PEP, as defined in the Hong Kong AML/CTF Laws;
- adverse media or other risk indicators suggest possible involvement in criminal activity, sanctions breaches, or other higher-risk behaviour; or
- any other factors arise that the Company considers relevant under its risk-based approach.

2.3. Customers shall undergo the following risk-based customer due diligence and KYC identification program, which may be conducted by the Company or by a KYC/AML Service Provider on its behalf:

- the customer creates a user account on the Platform;
- the customer uploads to his/her/its account the information and documents required under section 2.4(a)–(j);
- the information and documents submitted by the customer are transferred to a KYC/AML Service Provider for verification in accordance with section 2.4(k)–(l);
- the KYC/AML Service Provider reviews and verifies the information and documents provided;
- the KYC/AML Service Provider conducts screening of the customer against relevant sanctions, terrorism, PEP and other watchlists (collectively the “Watchlists Databases”);
- following verification and screening, the KYC/AML Service Provider either confirms or declines the customer;

- if the customer meets any of the higher-risk criteria under section 2.2, the Company will apply enhanced due diligence based on its risk-based approach or refuse to provide Services and will refund any funds previously advanced by the customer to the originating account, in the same form where practicable and within a reasonable period, unless otherwise provided in this Policy or required by applicable laws and regulations;
- the Company will request additional information and/or documents from customers from high-risk jurisdictions or where the information or documentation submitted indicates a higher risk of money laundering, terrorist financing, or sanctions exposure.

2.4. Once a customer has created a user account on the Platform, the following information and/or documents will be collected for all accounts and for any person (individual or legal entity) that is creating a new user account and whose name is on the account, before any Services are provided to that person:

(a) full legal name;

(b) date of birth (for individuals) or date of incorporation/registration (for legal entities);

(c) nationality (for individuals) or jurisdiction of incorporation/registration (for legal entities);

(d) residential address (for individuals) or registered office and principal place of business (for legal entities);

(e) valid government-issued identification document (e.g., passport, national ID card, Hong Kong identity card, or equivalent) for individuals;

(f) constitutional documents for legal entities (e.g., certificate of incorporation, business registration certificate, articles of association, register of directors and shareholders, where applicable);

(g) information on the beneficial owners of legal entities, including their identity documents and ownership/control structure;

(h) contact details (email address, phone number);

(i) information on the nature and purpose of the business relationship and the expected pattern of activity;

(j) any other information or documents that the Company considers reasonably necessary in light of its risk-based approach and the Hong Kong AML/CTF Laws;

(k) any electronic verification records, screening results and other outputs generated by the KYC/AML Service Providers;

(l) where applicable, additional documentation or confirmations requested to resolve discrepancies or mitigate specific risks.

2.5. Using risk-based procedures to verify and document all information received from the customer, the Company will make all reasonable efforts to form a reasonable belief that:

- it knows the true identity of the customer (and, for legal entities, their directors, shareholders, beneficial owners and any relevant related persons); and
- the information and documents provided by the customer are accurate, complete and up to date.

The Company and the KYC/AML Service Providers will analyze all information and documents received or collected from a customer to determine whether they are sufficient to form this reasonable belief. Customer identity may be verified through documentary and/or non-documentary means, including electronic and database-based verification. The Company may use any appropriate method of verification, taking into account the risks in each particular case and the standards set under the Hong Kong AML/CTF Laws.

2.6. If the Company and/or a KYC/AML Service Provider identifies information or circumstances that indicate possible money laundering, terrorist financing or other suspicious activity, the Company will:

- consider whether the activity is suspicious within the meaning of the Hong Kong AML/CTF Laws;
- where required, file a suspicious transaction report (STR) with the Joint Financial Intelligence Unit (JFIU) or any other competent Hong Kong authority, in accordance with applicable statutory requirements, without tipping off the customer; and
- take any additional measures required or permitted under the Hong Kong AML/CTF Laws, including freezing or restricting transactions, terminating the relationship, or otherwise reporting to relevant authorities.

2.7. Where the Company cannot form a reasonable belief that it knows the true identity of a customer (or, in the case of a legal entity, its directors, shareholders, beneficial owners and/or any related persons), the Company has the right to:

- deactivate the customer’s user account on the Platform;
- close the user account after reasonable attempts to verify the customer’s identity have failed;
- refund to the customer any funds previously advanced by such customer to the account from which they originated, in the same type and manner and within a reasonable time, unless otherwise provided in this Policy or required by applicable laws and regulations; and
- determine whether any reporting to competent authorities is required under the Hong Kong AML/CTF Laws.

2.8. If a potential or existing customer refuses to provide information or documents requested under this Policy, or if the Company reasonably believes or discovers that the customer has intentionally provided false, incorrect or misleading information, the Company has the right to deactivate the customer’s account and to consider closing any existing account.

2.9. Any funds previously deposited by such a customer will be refunded to the originating account in the same type and manner within a reasonable time, unless otherwise provided in this Policy or required by applicable laws and regulations.

3. Recordkeeping

3.1. The Company will keep and maintain logs of all verification steps, including:

- all identifying information and documents provided by the customer and third parties; and
- all steps, decisions and resolutions taken by the Company in the identification and verification process.

3.2. In particular, the Company will keep records containing:

- for documentary verification – all information and documents relied upon to identify and verify the customer's identity;
- for non-documentary verification – all information and logs describing the steps taken and the results obtained when verifying the customer's identity;
- for verification based on third-party service providers – information on the customer's verification status and logs/messages between the Company and such third parties in relation to that customer.

3.3. All information kept in relation to customer verification is confidential and will not be disclosed to any third party, except:

- as expressly provided in this Policy;
- as required or permitted under the Hong Kong AML/CTF Laws and other applicable laws and regulations; or
- to KYC/AML Service Providers and other professional advisers engaged by the Company, subject to appropriate confidentiality and data-protection safeguards.

3.4. Records will be retained for at least the minimum period required under the Hong Kong AML/CTF Laws (or any longer period determined by the Company), including for at least the prescribed number of years after the end of the business relationship or the date of the last transaction, whichever is later.

4. Additional customer verification and rejection rights

4.1. In compliance with applicable regulations, including the Hong Kong AML/CTF Laws, the Company may request any additional information necessary for verification and ongoing monitoring purposes. This may involve further checks and documentation to ensure adherence to the stringent requirements governing financial and commercial activities in Hong Kong.

4.2. The Company reserves the right, at its sole discretion, to reject any customer or to terminate any customer's access to the Company's Services without additional explanation, where it considers this necessary or appropriate under its risk-based approach or to comply with the Hong Kong AML/CTF Laws.

4.3. The Company reserves the right to use, or to require customers to use, external services for identity verification and compliance checks. The Company may also appoint external legal or compliance advisers to review and verify compliance data. These measures are aimed at maintaining high standards of due diligence and ensuring the integrity of the Company’s operations in preventing money laundering, terrorist financing and related criminal activities.

Last updated: 20.11.2025