SECURE
DIGITAL MARKETS

Know Your Customer Policy and Anti-Money Laundering Measures

For Secure Digital Markets ("**SDM**" or the "**Company**")

Objectives, Scope and Application of the Policy:

The primary objective is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities or terrorist financing activities.

- To lay down explicit criteria for acceptance of customers.
- To establish procedures to verify the bona-fide identification of individuals/non individuals for opening of account.
- To establish processes and procedures to monitor high value transactions and/or transactions of suspicious nature in accounts.
- To develop measures for conducting due diligence in respect of customers and reporting of such transactions.

Definition of Customer

For the purpose of Secure Digital Markets's KYC policy a 'Customer' is defined as a person or entity that maintains an account and/or has a business relationship with Secure Digital Markets; beneficiaries of transactions conducted by professional intermediaries such as Introducing Brokers (IB's), Account Managers, Money Managers or solicitors, as permitted under the law; or any person or entity connected with a financial transaction which can pose significant reputational or other risks to Secure Digital Markets.

Customer Acceptance Policy ("CAP")

The Customer Acceptance Policy requires all customers or potential customers to fill in the Secure Digital Markets Application Form to capture the relevant data for

all categories of customers and provide supporting documents as given in the form as a part of customer identification process / KYC.

Customer Identification Procedures ("CIP")

Customer identification means identifying the customer and verifying his/her identity by using reliable, independent, data or information. Secure Digital Markets shall obtain sufficient information necessary to verify the identity of each new customer along with brief details of its promoters and management, whether regular or occasional and the purpose of the intended nature of business relationship. The requirement as mentioned herein may be moderated according to the risk perception.

KYC Document requirements:

A. Proof of Identity in case of Individual

One *Self Attested* copy of any one of the following:

1. Passport
2. Driving License
3. ID card issued by any central/state govt.

B. Proof of Address in case of Individual

One *Self Attested* copy of any one of the following:

1. Passport
2. Telephone bill (Landline)
3. Electricity bill
4. Bank Account statement issued by a public sector bank (such statement being not older than one month from the date of application)

SECURE
DIGITAL MARKETS

C. Proof of Identity and Principal place of Business in case of non-Individuals

A certified true copy of **all** the below documents, duly signed and stamped by a Company Secretary or a Director of the applicant company:

1. Certificate of Incorporation
2. Certificate of Commencement of Business (if applicable)
3. Memorandum and Articles of Association
4. List of Directors
5. Latest shareholding structure
6. Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account
7. Power of Attorney granted to its managers, officers or employees to transact business on its behalf
8. Copy of the telephone bill (landline) of the principal place of business

If any of the above documents are in any language other than English, it must be translated into English along with a certificate from translator / notary public.

Important: Secure Digital Markets shall periodically review the risk categorization of loan assets, which shall not be less than once every 6 months. Secure Digital Markets will also periodically update the customer identification data after the account is opened. The review process shall not be less than once in five years in the case of low risk category customers, and not less than once every two years in case of high and medium risk categories.

Monitoring and reporting of Transactions:

Monitoring of transactions will be conducted taking into consideration the risk profile of the account. Secure Digital Markets shall make endeavors to understand the normal and reasonable activity of the customer so that the transactions that fall outside the regular/pattern of activity can be identified, Special attention will be paid to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose.

Background of the customer, country of origin, sources of funds, the type of transactions involved and other risk factors shall determine the extent of monitoring. Higher risk accounts shall be subject to intensified monitoring. Secure Digital Markets shall carry out the periodic review of risk categorization of transactions/customers and the need for applying enhanced due diligence measures at a periodicity of not less than once in six months.

Secure Digital Markets shall explore the possibility of validating the new accounts opening application with various watch lists available in public domain, including domestic and international anti-money laundering (AML) regulations, including the USA Patriot Act, The UK Bribery Act and the European Union Third Money Laundering Directive. After due diligence, any transactions of suspicious nature will be duly reported by principal officer to the Ministry of Justice or such person or authority as required by law.

To ensure monitoring and reporting of all transactions and sharing of information as required under the law, the Board may nominate any Director or authorized Compliance Officer or any other officer(s) duly authorized to be designated as Secure Digital Markets's Principal Officer with respect to KYC/ AML/ CFT.

Principal Officers for KYC/ AML/ CFT:

Principal Officer(s) for KYC will act independently and report directly to the concerned Director/ or to the Board of Directors. The role and responsibilities of the Principal Officer(s) should include overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Anti-Money Laundering and Countering Financing of Terrorism Act, 2009, rules and regulations made there under, as amended from time to time.

Closure of Accounts/Business Relationship:

Where Secure Digital Markets is unable to apply appropriate KYC measures due to non furnishing of information and/or non-operation by the customer, the Company shall terminate the Business Relationship after issuing due notice to the customer

explaining the reasons for taking such a decision. Such decision shall be taken with the approval of the Managing Director or Principal Officer.

Sanctioned Countries:

Canada has imposed sanctions and/or related measures against the following countries:

- Central African Republic
- Democratic Republic of the Congo
- Eritrea
- Iran
- Iraq
- Lebanon
- Libya
- Mali
- Myanmar
- North Korea
- Russia
- Somalia
- South Sudan
- Sudan
- Syria
- Tunisia
- Ukraine
- Venezuela
- Yemen
- Zimbabwe

SECURE
DIGITAL MARKETS

Restricted Businesses and Industries

Financial and professional services

Investment & credit services	Securities brokers; mortgage consulting or debt reduction services; credit counselling or repair; real estate opportunities; lending instruments
Money and legal services	Money transmitters, check cashing, wire transfers, money orders; currency exchanges or dealers; bail bonds; collections agencies; law firms collecting funds for any purpose other than to pay fees owed to the firm for services provided by the firm (e.g., firms cannot use Stripe to hold client funds, collection or settlement amounts, disputed funds, etc.)

IP Infringement, regulated or illegal products and services

Intellectual property or proprietary rights infringement	Sales, distribution, or access to counterfeit music, movies, software, or other licensed materials without the appropriate authorization from the rights holder; any product or service that directly infringes or facilitates infringement upon the trademark, patent, copyright, trade secrets, or proprietary or privacy rights of any third party

Counterfeit or unauthorized goods	Unauthorized sale or resale of brand name or designer products or services; sale of goods or services that are illegally imported or exported
Gambling	Lotteries; bidding fee auctions; sports forecasting or odds making; fantasy sports leagues with cash prizes; internet gaming; contests; sweepstakes; games of chance
Regulated or illegal products or services	Marijuana dispensaries and related businesses; sale of tobacco, e-cigarettes, and e-liquid; online pharmacies; age restricted goods or services; weapons and munitions; gunpowder and other explosives; fireworks and related goods; toxic, flammable, and radioactive materials; products and services with varying legal status on a state-by-state basis; goods or services, the sale of which is illegal under applicable law in the jurisdictions to which your business is targeted or directed
Adult content and services	Pornography and other obscene materials (including literature, imagery and other media); sites offering any sexually-related services such as prostitution, escorts, pay-per view, adult live chat features

Unfair, predatory, or deceptive practices

Get rich quick schemes	Investment opportunities or other services that promise high rewards
Mug shot publication or pay-to-remove sites	Platforms that facilitate the publication and removal of content (such as mug shots), where the primary purpose of posting such content is to cause or raise concerns of reputational harm
No-value-added services	Sale or resale of a service without added benefit to the buyer; resale of government offerings without authorization or added value; sites that we determine in our sole discretion to be unfair, deceptive, or predatory towards consumers

Products or services that are otherwise restricted by our financial partners

Aggregation	Engaging in any form of licensed or unlicensed aggregation of funds owed to third parties, factoring, or other activities intended to obfuscate the origin of funds
Drug paraphernalia	Any equipment designed for making or using drugs, such as bongs, vaporizers, and hookahs

High risk businesses	Bankruptcy lawyers; computer technical support; psychic services; travel reservation services and clubs; airlines; cruises; timeshares; prepaid phone cards, phone services, and cell phones; telemarketing, telecommunications equipment and telephone sales; drop shipping; forwarding brokers; negative response marketing; credit card and identity theft protection; the use of credit to pay for lending services; any businesses that we believe poses elevated financial risk, legal liability, or violates card network or bank policies; any business or organization that a. engages in, encourages, promotes or celebrates unlawful violence or physical harm to persons or property, or b. engages in, encourages, promotes or celebrates unlawful violence toward any group based on race, religion, disability, gender, sexual orientation, national origin, or any other immutable characteristic
Multi-level marketing	Pyramid schemes, network marketing, and referral marketing programs
Pseudo pharmaceuticals	Pharmaceuticals and other products that make health claims that have not been approved or verified by the applicable local and/or national regulatory body

Social media activity	Sale of Twitter followers, Facebook likes, YouTube views, and other forms of social media activity
Substances designed to mimic illegal drugs	Sale of a legal substance that provides the same effect as an illegal drug (e.g., salvia, kratom)
Video game or virtual world credits	Sale of in-game currency unless the merchant is the operator of the virtual world

General

Information collected from the Customer shall be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes. Secure Digital Markets shall therefore, ensure that information sought from the customer is relevant to the perceived risk, is not intrusive and is in conformity with the guidelines issued by Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

Risk Management:

All customers would be included under this policy with the exception when scheduled commercial banks and select regulated financial institutions.

Further, **Secure Digital Markets customers will be categorized based on perceived risk, into three categories – A, B & C.** Category C customers include low risk, Category B contains medium risk customers while Category A are high risk customers. None of the entities will be exempted from Secure Digital Markets's KYC procedure, irrespective of the status and relationship with the Company. The above requirement may be moderated according to the risk perception.

1. **High Risk – (Category A):** High risk customers typically include (a) firms with silent partners (b) politically exposed persons (PEPs) of foreign origin (c) non face to face to customers and (d) person with dubious reputation as per public information available.

2. **Medium Risk – (Category B):** Medium risk customers will include (a) non – resident customers, (b) high net worth individuals (c) trust, charitable organizations, non govt. organization (NGO), organizations receiving donations, and companies having closed family shareholding or beneficial ownership.

3. **Low Risk – (Category C):** Low risk individuals (other than high net worth) and entities whose identities and sources of wealth can be easily identified and all other persons not covered under above two categories.

The Business Development Manager (Relationship Manager with client company) in Secure Digital Markets shall obtain the required data/documents and other relevant information and credit risk profiles of the existing and new customers and apply various Anti Money Laundering measures keeping in view the risk involved in a transaction.

Risk Management Committee ("RMC"):

The Principal officer may submit the periodic report to the RMC if a need arises in case of high risk cases and which may require further guidance from Committee so they can assess the risk involved in the case of different customers on the basis of data collected by the business team. Depending on the requirement, services of an independent consultant having knowledge and background on the subject may be taken. Such issues of categorization shall be kept confidential and shall not be divulged to any third party irrespective of their relationship with the Company at any level of organization.

KYC for the Existing Accounts:

While the KYC guidelines will apply to all new customers, the same would be applied to existing customers on the basis of materiality and risk. However,

transactions in existing customers would be continuously monitored for any unusual pattern in the operation of the accounts.

As required under the Act and rules, information so collected for existing or new customers shall be properly retained and preserved for each customer. Profile of the customer may be prepared for quick reference as and when required. The information/documents so collected shall be treated as confidential and shall not be divulged for cross selling or for any other purpose.

Employee's Training:

Secure Digital Markets shall have an ongoing employee training program so that the team members are adequately trained in KYC/ AML/ CFT procedures. Training requirements shall have different focuses for frontline staff, compliance staff and officer/staff dealing with the new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them.

Review of KYC Policy of Company

CMD/MD/CEO of Secure Digital Markets will be authorized to amend/modify the KYC/ AML/ CFT Policy or such other related guidance notes of Company, to be in line with the FINTRAC or such other statutory authority's requirements/updates/ amendments from time to time.

MANDATORY DOCUMENTS REQUIRED FOR STARTING A RELATIONSHIP

A. Private and Public Limited Companies

1. Certificate of Incorporation
2. Certificate of commencement of business in case of Public Ltd. Company
3. Certified True copy (certified by Company Secretary or Director) of the Memorandum and Articles of Association.
4. List of Directors (certified by Company Secretary or Director)
5. True Copy (certified by Company Secretary or director) of list of signatories.

6. Evidence of listing in a stock exchange, if any

B. Accounts, where third party mandate exist

1. True notarized copy (with attested signature of POA holder and Managing Director or his authorized signatory) of power of Attorney (POA) Agreement.
2. Reason for granting POA.
3. True Copy (certified by Company Secretary or director) of Identity and Address documents of POA holder
4. All other verification documents as applicable for Public/Private limited companies.

C. Financial Institutions

1. True copy (certified by Company Secretary or director) of Certificate of Institution's License.
2. True copy (certified by Company Secretary or director) of Certificate of Incorporation.
3. True copy (certified by Company Secretary or director) of Statue or equivalent, stating that the institution is a regulated entity.
4. All other verification documents as applicable for Public/Private limited companies.

Acceptable proof of address documents (Any one)

1. Sales Tax Registration certificate
2. Recent (not more than 3 months old) utility bill in the name of the company (Telephone Bill, Electricity Bill, Water Bill, Lease Agreement duly signed by all parties, Rental Agreement duly signed by all parties)
3. Any other documents issued by Government showing Address.
4. In case of difference in the addresses provided by the company and the address proof, the Business Verification report should be carried out by approved Chartered Accountant and should contain the following:

1. Whether there is a signage outside the address that shows the entity's existence at that address.
2. What level of business activity is seen at the address?
3. How long the entity has been in existence at that address.
4. For cases, where the operating/trading address is different from the registered address, office verification will be done by Chartered Accountant, for trading address. Where the registered and trading address is same, no separate proof is required to be provided (Other than the confirmation by the Chartered Accountant/Business)