BLACK STAR BROKERAGE LIMITED

Anti-Money Laundering (AML) Program:

Compliance and Supervisory Procedures

1. Firm Policy

It is the policy of the firm to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements under the Anti-Money Laundering Act, 2014 (Act 874), Securities Industries Act 2016 (Act 929) and its implementing regulations.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Although cash is rarely deposited into securities accounts, the securities industry is unique in that it can be used to launder funds obtained elsewhere, and to generate illicit funds within the industry itself through fraudulent activities. Examples of types of fraudulent activities include insider trading, market manipulation, ponzi schemes, cybercrime and other investment-related fraudulent activity.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

Black Star Brokerage Ltd(BSB) AML policies, procedures and internal controls are designed to ensure compliance with all applicable regulations and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

2. AML Compliance Person Designation and Duties

BSB has designated a senior officer as its Anti-Money Laundering Program Compliance Person (AML Compliance Person), with full responsibility for the firm's

AML program. The designated officer has a working knowledge of the organization and its implementing regulations and is qualified by experience, knowledge and training. The duties of the AML Compliance Person will include monitoring the firm's compliance with AML obligations, overseeing communication and training for employees, and any other duties the firm will assign to him/her. The AML Compliance Person will also ensure that the firm keeps and maintains all of the required AML records and will ensure that Suspicious Activity Reports (SARs) are filed with the Financial Intelligence Unit when appropriate. The AML Compliance Person is vested with full responsibility and authority to enforce the firm's AML program.

We typically provide the appropriate authorities with contact information for the AML Compliance Person including: (1) name; (2) title; (3) mailing address; (4) email address; (5) telephone number. The firm will promptly notify the regulatory agencies of any change in this information and will review, and if necessary update, this information within 30 business days after the end of each calendar year.

3. AML Information

We will respond to a request from implementing agencies concerning accounts and transactions by immediately searching our records to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity or organization named in the Request.

If we search our records and do not find a matching account or transaction, then we reply to the request stating that we do not keep such records or we do not have in our records. We will maintain documentation that we have performed the

required search by maintaining a log showing the date of the request, the number of accounts searched, the name of the individual conducting the search and a notation of whether or not a match was found.

We will not disclose the fact that the enforcement agencies have requested or obtained information from us, except to the extent necessary to comply with the information request. The Compliance Officer will review, maintain and implement procedures to protect the security and confidentiality of requests.

4. Customer Identification Program

In addition to the information we must collect from our customers, we have established, documented and maintained a written Customer Identification Program (CIP). We will collect certain minimum customer identification information from each customer who opens an account; utilize risk-based measures to verify the identity of each customer who opens an account; record customer identification information and the verification methods and results; provide the required adequate CIP notice to customers that we will seek identification information to verify their identities; and compare customer identification information with government-provided lists of suspected terrorists, once such lists have been issued by the government.

a. Required Customer Information

Prior to opening an account, an officer responsible will collect the following information for all accounts, if applicable, for any person, entity or organization that is opening a new account and whose name is on the account:

(1) the name;

(2) date of birth (for an individual);

(3) an address, which will be a residential or business street address (for an individual), a Post Office (PO) box number, or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address), digital address, email address, phone number, or a principal place of business, local office, or other physical location (for a person other than an individual); and

(4) an identification number, which will be a taxpayer identification number , or one or more of the following: a taxpayer identification number, passport number and country of issuance, alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph.

b. Customers Who Refuse to Provide Information

If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, our firm will not open a new account and, after considering the risks involved, consider closing any existing account. In either case, our AML

Compliance Person will be notified so that we can determine whether we should report the situation to FIC.

c. Verifying Information

Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. The compliance officer will analyze the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the true identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies).

We will verify customer identity through documentary means, non-documentary means or both. We will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever necessary. We may also use non-documentary means, if we are still uncertain about whether we know the true identity of the customer. In verifying the information, we will consider whether the identifying information that we receive, such as the customer's name, street address, zip code, telephone number (if provided), date of birth and Social Security number, allow us to determine that we have a reasonable belief that we know the true identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies).

Appropriate documents for verifying the identity of customers include the following:

- For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; and

- For a person other than an individual, documents showing the existence of the entity, such as certificate of incorporation and regulation, a government-issued business license, a partnership agreement or a trust instrument.

We understand that we are not required to take steps to determine whether the document that the customer has provided to us for identity verification has been validly issued and that we may rely on a government-issued identification as verification of a customer's identity. If, however, we note that the document shows some obvious form of fraud, we must consider that factor in determining whether we can form a reasonable belief that we know the customer's true identity.

We will use the following non-documentary methods of verifying identity:

- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database or other source

- Checking references with other financial institutions; or

- Obtaining a financial statement.

We will use non-documentary methods of verification when:

(1) the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard;
(2) the firm is unfamiliar with the documents the customer presents for identification verification;
(3) the customer and firm do not have face-to-face contact; and
(4) there are other circumstances that increase the risk that the firm will be unable to verify the true identity of the customer through documentary means.

We will verify the information within a reasonable time before or after the account is opened. Depending on the nature of the account and requested transactions, we may refuse to complete a transaction before we have verified the information, or in some instances when we need more time, we may, pending verification, restrict the types of transactions or dollar amount of transactions. If we find suspicious information that indicates possible money laundering, terrorist financing activity, or other suspicious activity, we will, after internal consultation with the firm's AML Compliance Person, file a STR in accordance with applicable laws and regulations.

d. Lack of Verification

When we cannot form a reasonable belief that we know the true identity of a customer, we will do the following: (1) not open an account; (2) impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity; (3) close an account after attempts to verify a customer's

identity fail; and (4) determine whether it is necessary to file a STR in accordance with applicable laws and regulations.

e. Recordkeeping

We will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. We will keep records containing a description of any document that we relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we will retain documents that describe the methods and the results of any measures we took to verify the identity of a customer. We will also keep records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. We will retain records of all identification information for five years after the account has been closed; we will retain records made about verification of the customer's identity for five years after the record is made.

h. Reliance on Another Financial Institution for Identity Verification

We may, under the following circumstances, rely on the performance by another institution (including an affiliate) of some or all of the elements of our Customer Identification Programme with respect to any customer that is opening an account or has established an account or similar business relationship with the other financial institution to provide or engage in services, dealings or other financial transactions:

- when such reliance is reasonable under the circumstances;
- when the other financial institution is subject to a rule implementing the anti-money laundering compliance program requirements and
- when the other financial institution has entered into a contract with our firm requiring it to certify annually to us that it has implemented its anti-money laundering program and that it will perform (or its agent will perform) specified requirements of the customer identification program.

5. Customer Due Diligence Rule

In addition to the information collected under the written Customer Identification Program, we have established, documented and maintained written policies and procedures reasonably designed to identify and verify beneficial owners of legal entity customers and comply with other aspects of the Customer Due Diligence (CDD) Rule. We will collect certain minimum CDD information from beneficial owners of legal entity customers. We will understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile. We will conduct ongoing monitoring to identify and report suspicious transactions, and, on a risk basis, maintain and update customer information.

a. Identification and Verification of Beneficial Owners

At the time of opening an account for a legal entity customer, we will identify any individual that is a beneficial owner of the legal entity customer by identifying any

individuals who directly or indirectly own 25% or more of the equity interests of the legal entity customer, and any individual with significant responsibility to control, manage, or direct a legal entity customer. The following information will be collected for each beneficial owner:

(1) the name;

(2) date of birth (for an individual);

(3) an address, which will be a residential or business street address (for an individual), or a Post Office (PO) box number, or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address); and

(4) an identification number, which will be a Social Security number, or one or more of the following: a passport number and country of issuance, or other similar identification number, such as an alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard.

For verification, we will describe any document relied on (noting the type, any identification number, place of issuance and, if any, date of issuance and expiration). We will also describe any non-documentary methods and the results of any measures undertaken.

b. Understanding the Nature and Purpose of Customer Relationships

We will understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile through the following methods.

Depending on the facts and circumstances, a customer risk profile may include such information as:

- *The type of customer;*
- *The account or service being offered;*
- *The customer's income;*
- *The customer's net worth;*
- *The customer's domicile;*
- *The customer's principal occupation or business; and*
- *In the case of existing customers, the customer's history of activity.*

c. Conducting Ongoing Monitoring to Identify and Report Suspicious Transactions

We will conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, maintain and update customer information, including information regarding the beneficial ownership of legal entity customers, using the customer risk profile as a baseline against which customer activity is assessed for suspicious transaction reporting.

6. Refugees and Asylum Seekers

BSB has put in place a system whereby refugees could open account even if they could not satisfy the KYC requirements. BSB will open account for refugees and asylum seekers using the following documents:

- A letterhead and the stamp of a Ghana immigration authority, the document containing the personal details of the refugee (name, place and date of birth, nationality and address); a photograph of the applicant.
- A letter mentioning their arrival in Ghana from the immigration authority.

7. Monitoring Accounts for Suspicious Activity

We will monitor account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to our business. (Red flags are identified below. The customer risk profile will serve as a baseline for assessing potentially suspicious activity. The AML Compliance Person or his or her designee will be responsible for this monitoring, will review any activity that our monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities.

The AML Compliance Person or his or her designee will conduct an appropriate investigation and review relevant information from internal or third-party sources before a STR is filed.

b. Red Flags

Red flags that signal possible money laundering or terrorist financing include, but are not limited to:

Customers – Insufficient or Suspicious Information

- Provides unusual or suspicious identification documents that cannot be readily verified.

- Reluctant to provide complete information about nature and purpose of business, prior banking relationships, anticipated account activity, officers and directors or business location.

- Refuses to identify a legitimate source for funds or information is false, misleading or substantially incorrect.

- Background is questionable or differs from expectations based on business activities.

- Customer with no discernable reason for using the firm's service.

Efforts to Avoid Reporting and Recordkeeping

- Reluctant to provide information needed to file reports or fails to proceed with transaction.

- Tries to persuade an employee not to file required reports or not to maintain required records.

- "Structures" deposits, withdrawals or purchase of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements.

- Unusual concern with the firm's compliance with government reporting requirements and firm's AML policies.

Certain Funds Transfer Activities

- Wire transfers to/from financial secrecy havens or high-risk geographic location without an apparent business reason.

- Many small, incoming wire transfers or deposits made using checks and money orders. Almost immediately withdrawn or wired out in manner inconsistent with customer's business or history. May indicate a Ponzi scheme.

- Wire activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent business purpose.

Certain Deposits or Dispositions of Physical Certificates

- Physical certificate is titled differently than the account.

- Physical certificate does not bear a restrictive legend, but based on history of the stock and/or volume of shares trading, it should have such a legend.

- Customer's explanation of how he or she acquired the certificate does not make sense or changes.

- Customer deposits the certificate with a request to journal the shares to multiple accounts, or to sell or otherwise transfer ownership of the shares.

Certain Securities Transactions

- Customer engages in prearranged or other non-competitive trading, including wash or cross trades of illiquid securities.

- Two or more accounts trade an illiquid stock suddenly and simultaneously.

- Customer journals securities between unrelated accounts for no apparent business reason.

- Customer has opened multiple accounts with the same beneficial owners or controlling parties for no apparent business reason.

•. Customer transactions include a pattern of receiving stock in physical form or the incoming transfer of shares, selling the position and wiring out proceeds.

- Customer's trading patterns suggest that he or she may have inside information.

Transactions Involving Penny Stock Companies

- Company has no business, no revenues and no product.

- Company has experienced frequent or continuous changes in its business structure.

- Officers or insiders of the issuer are associated with multiple penny stock issuers.

- Company undergoes frequent material changes in business strategy or its line of business.

- Officers or insiders of the issuer have a history of securities violations.

- Company has not made disclosures in SEC or other regulatory filings.

- Company has been the subject of a prior trading suspension.

Transactions Involving Insurance Products

- Cancels an insurance contract and directs funds to a third party.

- Structures withdrawals of funds following deposits of insurance annuity checks signaling an effort to avoid reporting requirements.

- Rapidly withdraws funds shortly after a deposit of a large insurance check when the purpose of the fund withdrawal cannot be determined.

- Cancels annuity products within the free look period which, although could be legitimate, may signal a method of laundering funds if accompanied with other suspicious indicia.

- Opens and closes accounts with one insurance company then reopens a new account shortly thereafter with the same insurance company, each time with new ownership information.

- Purchases an insurance product with no concern for investment objective or performance.

- Purchases an insurance product with unknown or unverifiable sources of funds, such as cash, official checks or sequentially numbered money orders.

Activity Inconsistent With Business

- Transactions patterns show a sudden change inconsistent with normal activities.

- Unusual transfers of funds or journal entries among accounts without any apparent business purpose.

- Maintains multiple accounts, or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.

- Appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.

Other Suspicious Customer Activity

- Unexplained high level of account activity with very low levels of securities transactions.

- Funds deposits for purchase of a long-term investment followed shortly by a request to liquidate the position and transfer the proceeds out of the account.

- Law enforcement subpoenas.

- Large numbers of securities transactions across a number of jurisdictions.

- Buying and selling securities with no purpose or in unusual circumstances (*e.g.*, churning at customer's request).

- Payment by third-party check or money transfer without an apparent connection to the customer.

- Payments to third-party without apparent connection to customer.

- No concern regarding the cost of transactions or fees (*i.e.*, surrender fees, higher than necessary commissions, etc.).

c. Responding to Red Flags and Suspicious Activity

When an employee of the firm detects any red flag, or other activity that may be suspicious, he or she will notify the Compliance Officer. Under the direction of the AML Compliance Person, the firm will determine whether or not and how to further

investigate the matter. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account and/or filing a STR.

7. Suspicious Transactions Reporting

.

a. Filing a STR

We will file STRs with appropriate authorities for any transactions (including deposits and transfers) conducted or attempted by, at or through our firm involving GHS50,000 or more of funds or assets (either individually or in the aggregate) where we know, suspect or have reason to suspect:

(1) the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade any law or regulation or to avoid any transaction reporting requirement under the applicable law or regulation;

(2) the transaction is designed, whether through structuring or otherwise, to evade any requirements of the AML regulations;

(3) the transaction has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and after examining the background, possible purpose of the transaction and other facts, we know of no reasonable explanation for the transaction; or

(4) the transaction involves the use of the firm to facilitate criminal activity.

We will also file a STR and notify the appropriate law enforcement authorities (SEC & FIC) in situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes. In addition, although we are not required to, we may contact SEC or FIC in cases where a STR we have filed may require immediate attention by the SEC or FIC.

.

We will report suspicious transactions by completing a STR, and we will collect and maintain supporting documentation as required by the AML regulations.

We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the AML regulations. We understand that anyone who is subpoenaed or required to disclose a STR or the information contained in the STR will, except where disclosure is requested by the SEC, or another appropriate law enforcement or regulatory agency, decline to produce the STR or to provide any information that would disclose that a STR was prepared or filed. We will notify the appropriate law enforcement authority of any such request and our response.

8. AML Recordkeeping

a. Responsibility for Required AML Records and SAR Filing

Our AML Compliance Person and his or her designee will be responsible for ensuring that AML records are maintained properly and that STRs are filed as required.

In addition, as part of our AML program, our firm will create and maintain STRs and relevant documentation on customer identity and verification and funds transmittals. We will maintain STRs and their accompanying documentation for at least five years. We will keep other documents according to existing AML and other recordkeeping requirements.

b. SAR Maintenance and Confidentiality

We will hold STRs and any supporting documentation confidential. We will not inform anyone outside of law enforcement or regulatory agencies about a STR. We will refuse any subpoena requests for STRs or for information that would disclose that a STR has been prepared or filed and immediately notify the law enforcement or regulatory agencies of any such subpoena requests that we receive. We will segregate STR filings and copies of supporting documentation from other firm books and records to avoid disclosing STR filings. Our AML Compliance Person will handle all subpoenas or other requests for STRs.

9. Training Programs

We will develop ongoing employee training under the leadership of the AML Compliance Person and senior management. Our training will occur on at least an annual basis. It will be based on our firm's size, its customer base, and its resources and be updated as necessary to reflect any new developments in the law.

Our training will include, at a minimum: (1) how to identify red flags and signs of money laundering that arise during the course of the employees' duties; (2) what to do once the risk is identified (including how, when and to whom to escalate

unusual customer activity or other red flags for analysis and, where appropriate, the filing of STRs); (3) what employees' roles are in the firm's compliance efforts and how to perform them; (4) the firm's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with the AML/CFT.

We will develop training in our firm, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures and explanatory memos. We will maintain records to show the persons trained, the dates of training and the subject matter of their training.

We will review our operations to see if certain employees, such as those in compliance, margin and corporate security, require specialized additional training. Our written procedures will be updated to reflect any such changes.

10. Program to Independently Test AML Program

a. Staffing

The testing of our AML program will be performed at least annually (on a calendar year basis) by an independent third party. We will evaluate the qualifications of the independent third party to ensure they have a working knowledge of applicable requirements under the AML and its implementing regulations. Independent testing will be performed more frequently if circumstances warrant.

b. Evaluation and Reporting

After we have completed the independent testing, staff will report its findings to senior management. We will promptly address each of the resulting recommendations and keep a record of how each noted deficiency was resolved.

11. Monitoring Employee Conduct and Accounts

We will subject employee accounts to the same AML procedures as customer accounts, under the supervision of the AML Compliance Person. We will also review the AML performance of supervisors, as part of their annual performance review. The AML Compliance Person's accounts will be reviewed the CEO.

12. Financial inclusion

Black Star Brokerage Limited has put in place an outreach programme that seeks to educate the public on financial literacy. Additionally, measures such as "alternative documentary evidence of personal identity and address" has been put in place for the identification of the financially excluded in society in order to provide access to financial services to them.

In situations where we have reasonable grounds to conclude that an individual client is not able to produce the detailed evidence of his identity and cannot reasonably be expected to do so, we accept as identification evidence of a letter or statement from a person in a position of responsibility who knows the client and

can confirm that the client is who he/she says he/she is, including confirmation of his permanent address. The ID of the guarantor must be obtained and verified.

The internal procedures also include maintaining a file with the reasons for doing so along with the account opening documents.

13. Closure of Clients' Accounts

The client may request Black Star Brokerage Ltd by giving 7 days' prior notice in writing to suspend his account temporarily.

Black Star Brokerage Ltd may suspend/close the client account, if BSB observes any abnormal or suspicious activity in the client account through its monitoring and surveillance of the client account. BSB may also at any time, suspend or close the client account due to any action from the regulatory agencies. Further, BSB may also temporarily suspend/close the client account if there is no activity in the client account for a period of 24 months, as deemed fit by BSB from time to time. Also, BSB can withhold the payouts of client and suspend his/her trading account due to his surveillance action or judicial or/any regulatory order/action requiring client suspension.

All losses to the client on account of the above shall be borne solely by the client and BSB shall not be responsible for the same. In case of any claim against BSB, the Client shall indemnify BSB in this regard.

14. Employee Screening

As part of the employee selection process, Black Star Advisors has established a Know Your Employee policy to ascertain the background, conflict of interests and vulnerabilities of employees to money laundering.

The policy includes, but not limited to the background screening of employees for criminal history, verification of education and professional qualifications.

There is zero tolerance for Employees who engage in fraudulent activities. Such persons shall be deemed unfit to work with the Company and their appointment terminated.

15. Confidential Reporting of AML Non-Compliance

Employees will promptly report any potential violations of the firm's AML compliance program to the AML Compliance Person, unless the violations implicate the AML Compliance Person, in which case the employee shall report to the board. Such reports will be confidential, and the employee will suffer no retaliation for making them.

16. Additional Risk Areas

The firm has reviewed all areas of its business to identify potential money laundering risks that may not be covered in the procedures described above.

17. Senior Manager Approval

This program is compiled and approved by the Board. Subsequent amendments will be approved by the CEO or Head of Compliance.