BITS1002 GREATER HOUSTON, LLC

Anti-Money Laundering (AML) and Know Your Client (KYC) Policy

LAST REVISED: March 31, 2025

1. Company Policy

It is the Anti-Money Laundering (AML) and Know Your Client (KYC) policy of BITS1002 Greater Houston, LLC, a Wyoming-based company (hereinafter referred to as “the company”) 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 law and implementing regulations within the company’s existing projects.

Money laundering is defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have been 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.

Our AML policies, procedures, and internal controls are designed to ensure compliance with all applicable regulations and authorized body rules 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

The company may designate a compliance officer as its Anti-Money Laundering Program Compliance Person (AML Compliance Person), with full responsibility for the company’s AML program. The company’s director or board of directors shall appoint a compliance

officer. The duties of the AML Compliance Person, if designated, will include monitoring the company's compliance with AML obligations, overseeing communication and training for employees, and any other duties decided by the director. The AML Compliance Person will also ensure that the company keeps and maintains all of the required AML records and will ensure that Suspicious Activity Reports (SARs) are filed with the authorized body when appropriate. The AML Compliance Person is vested with full responsibility and authority to enforce the company's AML program. In cases where internal resources are limited, the company may recognize the value of third-party compliance solutions and delegate the role of AML Compliance Person to external service providers, who bring specialized knowledge and advanced compliance tools.

3. Provision of AML Information to authorized bodies and Financial Institutions

We will respond to an authorized body request 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 relevant request. We have 14 days (unless otherwise specified by the respective authorized body) from the transmission date of the request to respond to a request.

If the compliance officer searches our records and does not find a matching account or transaction, then the compliance officer might not reply to the request. We will maintain documentation proving that we have performed the required search by printing a self-verification document confirming that we have searched the subject information against our records OR maintain 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 authorized body has 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 from the authorized bodies similar to those procedures established to satisfy the requirements of the law with regard to the protection of users' nonpublic information.

We will direct any questions we have about the request to the law enforcement agency as designated in the request.

In addition to the information, we must collect under the laws of the jurisdictions where the company operates its projects, we have established a KYC Program. We will collect certain minimum customer identification information from each customer who opens an account for any of our projects; utilize risk-based measures to verify the identity of each.

Unless otherwise stated in the Request, we will not be required to treat the information request as continuing in nature, and we will not be required to treat the periodic Requests as a government provided a list of suspected terrorists for purposes of the customer identification and verification requirements.

We will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, for the authorized bodies, by segregating it from the company's other books and records.

We also will employ procedures to ensure that any information received from another

institution shall not be used for any purpose other than:

- identifying and, where appropriate, reporting on money laundering or terrorist activities;
- determining whether to establish or maintain an account or to engage in a transaction;
- assisting the financial institutions in complying with performing such activities.

4. Checking the Office of Foreign Assets Control Listings

Before opening an account, and on an ongoing basis, the compliance officer will check to ensure that a customer does not appear on the Specially Designated Nationals and Blocked Persons ("SDN") list or is not engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by the authorized body. Because the list and listings of economic sanctions and embargoes are updated frequently, we will consult them on a regular basis and subscribe to receive any available updates when they occur. With respect to the SDN list, we may also access that list through various software programs to ensure speed and accuracy. The compliance officer will also review existing accounts against the SDN list and listings of current sanctions and embargoes when they are updated, and the compliance officer will document the review.

If we determine that a customer is on the SDN list or is engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by an authorized body, we will reject the transaction and/or block the customer's assets and file blocked assets and/or rejected transaction form with the authorized body within 10 days.

5. Know Your Customer

In addition to the information, we must collect under the laws of the jurisdictions where the company operates its projects, we have established a KYC Program. We will collect certain minimum customer identification information from each customer who opens an account for any of our projects; 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 KYC 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 or respective international authority.

5.1 Required Customer Information

Prior to opening an account for any of its projects, Company will collect the following information for such accounts, if applicable, for any person, entity, or organization that is opening a new account and whose name is on the account:

(1) full 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 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), or a principal place of business, local office, or other physical location (for entities); and

(4) an identification number, which may be:

a) national or international ID (which must not expire within the next 3 months of the submission date);

b) a taxpayer identification number,

c) driver's license (national or international);

d) any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard.

(5) customer's contact telephone number and e-mail address;

(6) Customer Binance Smart Chain wallet address under which, in combination with the information collected above, we will be able to identify any of our customers and the transactions they make within our projects.

(7) information to prove their status as accredited investors.

With regard to the customers who are the legal entities, in addition to point (3) above, we will collect the following information/documents:

(8) statutory documents;

(9) description of their corporate structure;

(10) information on their beneficial owners and core management (directors or members of the board of directors);

(11) documents from their local financial institutions (e.g., banks) to prove their financial credibility and good reputation.

When opening an account for a foreign business or enterprise that does not have an identification number, we will request alternative government-issued documentation certifying the existence of the business or enterprise.

5.2 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, the company 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 the authorized body.

5.3 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 or the engaged third-party AML/KYC compliance services providers 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 safeguards, 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 certified articles of incorporation, 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 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 another source;
- Checking references with other financial institutions; or
- Obtaining a financial statement.
- and other non-documentary methods, if applicable.

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 company is unfamiliar with the documents the customer presents for identification verification;

(3) the customer and company do not have face-to-face contact; and

(4) other circumstances increase the risk that the company 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 money 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 company's AML Compliance Person, file a SAR in accordance with applicable laws and regulations.

5.4 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; or (4) determine whether it is necessary to file a SAR in accordance with applicable laws and regulations.

5.5 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.

5.6 Comparison with Government-Provided Lists of Terrorists

At such time as we receive notice that a respective governmental or international agency has issued a list of known or suspected terrorists and identified the list as a list for KYC purposes, we will, within a reasonable period of time after an account is opened (or earlier, if required by another law or regulation or directive issued in connection with an applicable list), determine whether a customer appears on any such list of known or suspected terrorists or terrorist organizations issued by any government agency and designated as such by functional regulators. We will follow all directives issued in connection with such lists.

We will continue to comply separately with rules prohibiting transactions with certain foreign countries or their nationals.

5.7 Notice to Customers

We will provide notice to customers that the company is requesting information from them to verify their identities, as required by law. We will use the following method to provide notice to customers: online.

5.8 Reliance on Another Financial Institution for Identity Verification.

We may, under the following circumstances, rely on the performance by another financial institution (including an affiliate) of some or all of the elements of our KYC 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 is regulated by a functional regulator; and
- when the other financial institution has entered into a contract with our company 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.

6. Travel Rule

The Travel Rule applies the FATF's wire transfer requirements (FATF Recommendation 16) to the virtual assets (VAs) context. The Travel Rule requires Virtual Asset Service Providers (VASPs) and financial institutions to obtain, hold, and transmit specific originator and beneficiary information immediately and securely when transferring VAs.

Although the Company will not be registered as a VASP, transactions with Tokens can sometimes involve regulated VASPs. Investors should be aware that in such instances VASPs would have to apply the travel rule.

7. Customer Due Diligence Rule

In addition to the information collected under the law, 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 as described above. 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.

7.1 Identification and Verification of Beneficial Owners

At the time of opening an account for a legal entity customer, the compliance officer 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 the residential or business street address of a next of kin or another contact individual (for an individual who does not have a residential or business street address), 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 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.

7.2 Identification and verification of the politically exposed persons (PEPs)

At the time of opening an account for an individual or legal entity customer, the

compliance officer will identify any individual that is a politically exposed person or has a relation to a politically exposed person.

In such a case the compliance officer will communicate with a customer who has identified him as PEP or has a relation to PEP for clarification of his/her purpose of utilization of the company's project(-s) and request additional documents and information from the respective financial institutions where such PEP or a person related to PEP is a client.

As regards the legal entities, our compliance officer or a third-party KYC/AML compliance services provider will identify PEPs in management or beneficiaries of such legal entities during the KYC verification procedure. In such a case our compliance officer will contact the legal entity to retain additional information on respective PEPs.

7.3 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 legal methods.

7.4 Conducting Ongoing Monitoring to Identify 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.

8. 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. 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 conducted, 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 SAR is filed.

8.1 Emergency Notification to Law Enforcement by Telephone

In situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, we will immediately call an appropriate law enforcement authority. If we notify the appropriate law enforcement authority of any such activity, we must still file a timely SAR.

8.2 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 the 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 that is false, misleading, or incorrect.
- The background is questionable or differs from expectations based on business activities.
- Customer with no discernible reason for using the Company's service.

Efforts to Avoid Reporting and Recordkeeping

- Reluctant to provide the information needed to file reports or fails to proceed with the transaction.
- Try to persuade an employee not to file required reports or not to maintain required records.
- Unusual concern with the Company's compliance with government reporting requirements and the Company's AML policies.

Certain Funds Transfer Activities

- Crypto/wire transfers to/from the customer's account in unusually large amounts or without an apparent reason.
- Crypto/wire activity that is unexplained, repetitive, unusually large, or shows unusual patterns or with no apparent business purpose.

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.
- A customer has opened multiple accounts with the same beneficial owners or controlling parties for no apparent business reason.
- Customer's trading patterns suggest that he or she may have inside information.

Other Suspicious Customer Activity

- Unexplained high-level of account-activity with exceptionally low levels of securities transactions.
- Law enforcement subpoenas.
- Large numbers of crypto/securities transactions across a number of jurisdictions.
- Buying and selling crypto/securities with no purpose or in unusual circumstances (e.g., churning at customer's request).
- No concern regarding the cost of transactions or fees (i.e., surrender fees, higher than necessary commissions, etc.).

8.4 Responding to Red Flags and Suspicious Activity

When an authorized employee of the company 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 company 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 SAR.

9. Suspicious Transactions and Reporting

Filing a SAR

We will file SARs with the authorized body for any transactions (including transfers) conducted or attempted by, at, or through our company (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 to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade law or regulation or to avoid any transaction reporting requirement under law or regulation;

(2) the transaction is designed, whether through structuring or otherwise, to evade any requirements of the authorized body 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, the 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 company to facilitate criminal activity.

We will also file a SAR and notify the appropriate law enforcement authority in situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes.

We may file a voluntary SAR for any suspicious transaction that we believe is relevant to the possible violation of any law or regulation but that is not required to be reported by us under the SAR rule. It is our policy that all SARs will be reported regularly to the Board of Directors and appropriate senior management, with a clear reminder of the need to maintain the confidentiality of the SAR.

We will report suspicious transactions by completing a SAR, and we will collect and maintain supporting documentation as required by the authorized body regulations. We will file a SAR-SF no later than 30 calendar days after the date of the initial detection of the facts that constitute a basis for filing a SAR. If no suspect is identified on the date of initial detection, we may delay filing the SAR for an additional 30 calendar days pending identification of a suspect, but in no case will the reporting be delayed more than 60 calendar days after the date of initial detection. The phrase “initial detection” does not mean the moment a transaction is highlighted for review. The 30-day (or 60-day) period begins when an appropriate review is conducted, and a determination is made that the transaction under review is “suspicious” within the meaning of the SAR requirements. A review must be initiated promptly upon identification of unusual activity that warrants investigation.

We will retain copies of any SAR filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the SAR. We will identify and maintain supporting documentation and make such information available to the authorized body, any other appropriate law enforcement agencies, state securities regulators, or upon request.

We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the authorized body regulations. We understand that anyone who is subpoenaed or required to disclose a SAR or the information contained in the SAR will, except where disclosure is requested by appropriate law enforcement or regulatory agency, decline to produce the SAR or to provide any information that would

disclose that a SAR was prepared or filed. We will notify the authorized body of any such request and our response.

We will maintain records of the following information:

(1) the name of the purchaser;

(2) the date of purchase;

(3) the type(s) of instrument(s) purchased;

(4) the hash number(s) of each of the instrument(s) purchased; and

(5) the amount of money for each of the instrument(s) purchased.

(6) We may ask about additional documents.

(7) We shall keep records required to be kept for five years, and such records shall be made available to the state authorities upon request at any time.

10. AML Recordkeeping

10.1 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 SARs are filed as required. In addition, as part of our AML program, our company will create and maintain SARs and relevant documentation on customer identity and verification and funds transmittals. We will maintain SARs and their accompanying documentation for at least five years. We will keep other documents according to existing regulations and other recordkeeping requirements, including certain rules that require retention periods.

10.2 SAR Maintenance and Confidentiality

We will hold SARs and any supporting documentation confidential. We will not inform anyone outside of appropriate law enforcement or regulatory agencies about SAR. We will refuse any subpoena requests for SARs or for information that would disclose that a SAR has been prepared or filed and immediately notify the authorized body of any such subpoena requests that we receive. We will segregate SAR filings and copies of supporting documentation from other company books and records to avoid disclosing SAR filings. Our AML Compliance Person will manage all subpoenas or other requests for SARs. We may share information with another financial institution about suspicious transactions in order to determine whether we will jointly file a SAR. In cases in which we file a joint SAR for a transaction that has been managed both by us and another financial institution, both financial institutions will maintain a copy of the filed SAR.

11. Applicable laws

In order to be compliant with the AML/KYC regulations, we apply both national and international regulations.

We monitor the changes in the applicable laws on an annual basis and, if necessary, amend our policies and procedures accordingly.

12. Company Relationships

We will work closely with the authorized body to detect money laundering. We will exchange information, records, data, and exception reports as necessary to comply with AML laws. Our company will have filed (and kept updated) the necessary annual certifications for such information. As a general matter, we will obtain and use the

following exception reports offered by our authorized body in order to monitor customer activity and we will provide the authorized body with proper customer identification and due diligence information as required to successfully monitor customer transactions. We have discussed how each company will apportion customer and transaction functions and how we will share information and set forth our understanding in a written document. We understand that the apportionment of functions will not relieve either of us of our independent obligation to comply with AML laws, except as specifically allowed under the authorized body and its implementing regulations.

13. 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 company'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 employee's 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 SARs); (3) what employees' roles are in the company's compliance efforts and how to perform them; (4) the company's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with the regulations. We will develop training in our company, 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.

14. 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 director will review the AML Compliance Person's accounts.

15. Confidential Reporting of AML Non-Compliance

Employees will promptly report any potential violations of the company'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 director. Such reports will be confidential, and the employee will suffer no retaliation for making them.

16. Additional Risk Areas

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