ALFALAH GHP INVESTMENT MANAGEMENT LIMITED

ANTI FRAUD POLICY

VERSION 1.0

1. Introduction:

Fraud can be devastating to any business and finding ways to prevent and detect fraud has become a top priority in today's environment. Building fraud awareness within the organization and developing a proactive antifraud program is a key to winning the battle.

This Anti-Fraud Policy aims to develop a culture across the company which raises awareness of the risks and consequences of fraud. It provides a framework for promoting the companies policies and procedures to prevent and detect fraud.

This policy covers fraud and loss within the company and applies to staff, investors and suppliers.

2. Definitions of Fraud:

In law, the term used to describe Fraud are such acts as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion. For practical purposes fraud may be defined as the:

"use of deception with the intention of obtaining an advantage, avoiding an obligation or causing loss to another party".

Merriam-Webster's Dictionary of Law defines meaning of Fraud as:

> "any act, expression, omission, or concealment calculated to deceive another to his or her disadvantage; specifically: a misrepresentation or concealment with reference to some fact material to a transaction that is made with knowledge of its falsity or in reckless disregard of its truth or falsity and with the intent to deceive another and that is reasonably relied on by the other who is injured thereby"

Computer fraud is where information technology equipment has been used to manipulate programs or data dishonestly (for example, by altering, substituting or destroying records, or creating spurious records), or where the use of an IT system was a material factor in the perpetration of fraud. Theft or fraudulent use of computer time and resources, including unauthorised personal browsing on the internet, is included in this definition.

International Standard on Auditing 240 describes term fraud as an intentional act by one or more individuals among management, those charged with governance, employees or third parties, involving the use of deception to obtain an unjust or illegal advantage. Fraud involving one or more members of management is referred as "management fraud"; fraud involving only employees of the entity is referred to as "employee fraud"

3. So, What Is Fraud?

Fraud is a broad concept that refers generally to any intentional act committed to secure unfair or unlawful gains. Financial fraud typically falls into four broad categories:

- **Fraudulent financial reporting** — Most fraudulent financial reporting schemes involve earnings management, arising from improper revenue recognition, and overstatement of assets or understatement of liabilities.
- **Misappropriation of assets** — This category involves external and internal schemes, such as embezzlement, payroll fraud and theft.

- **Expenditures and liabilities for improper purposes** — This category refers to commercial and public bribery, as well as other improper payment schemes.

- **Fraudulently obtained revenue and assets, and costs and expenses avoided** — This category refers to schemes where an entity commits a fraud against its employees or third parties, or when an entity improperly avoids an expense, such as tax fraud.

4. Alfalah GHP Investment Management Limited (AGIM) Policy on Fraud:

Alfalah GHP Investment Management Limited requires all staff at all times to act honestly and with integrity and to safeguard the company's & investors resources for which they are responsible. The AGIM will not accept any level of fraud or corruption; consequently, any case will be thoroughly investigated and dealt with appropriately. The AGIM is committed to ensuring that opportunities for fraud and corruption are reduced to the lowest possible level of risk.

AGIM understands that risk of fraud can be reduced through a combination of prevention, deterrence, and detection measures. However, management is also aware that fraud can be difficult to detect because it often involves concealment through falsification of documents or collusion among management, employees, or third parties. Therefore, AGIM places importance to a strong emphasis on fraud prevention, which may reduce opportunities for fraud to take place, and fraud deterrence, which could persuade individuals that they should not commit fraud because of the likelihood of detection and punishment. Moreover, prevention and deterrence measures are much less costly than the time and expense required for fraud detection and investigation.

5. ANTIFRAUD PROGRAMS AND CONTROLS

The Policy identifies measures the management will implement to prevent, deter, and detect fraud. These measures are based on three fundamental elements. Broadly stated, these fundamental elements are:

1) create and maintain a culture of honesty and high ethics;
2) evaluate the risks of fraud and implement the processes, procedures, and controls needed to mitigate the risks and reduce the opportunities for fraud; and
3) develop an appropriate oversight process.

6. CREATING A CULTURE OF HONESTY AND HIGH ETHICS

It is the responsibility of the management to create a culture of honesty and high ethics and to clearly communicate acceptable behaviour and expectations of each employee.

Creating a culture of honesty and high ethics includes the following.

- Setting the Tone at the Top
- Developing Code of Conduct/Ethics
- Creating a Positive Workplace Environment
- Hiring and Promoting Appropriate Employees

a. **Setting the Tone at the Top:**

It is the responsibility of the senior management of the company to set the "tone at the top" for ethical behaviour within the organization. It is necessary for management to both behave ethically and openly communicate its expectations for ethical behaviour because most employees are not in a position to observe management's actions. Management must show employees through its words and actions that dishonest or unethical behaviour will not be tolerated, even if the result of the action benefits the entity. Moreover, it should be evident that all employees are treated equally, regardless of their position.

b. **Code of Conduct / Ethics**

The cornerstone of an effective antifraud environment is a culture with a strong value system founded on integrity. This value system is reflected in a code of conduct / ethics.

AGIM has approved code of conduct and ethics in its first board meeting the code applies to all staff/Officers including CEO, Head of Department, Senior Manager, Managers and Executive/Officers. All employees are required to act within the organization's code of conduct. The code outlines specific topics that the must follows.

(1) Code of Conduct - Disposition in Corporate and Professional Matters
(2) Code of Conduct - Handling Sensitive Information
(3) Code of Conduct - Personal Affairs
(4) Code of Conduct - Personal Disposition
(5) Confidentiality
(6) Personal Share Dealing Policy
(7) Code Of Conduct – Sales And Marketing Of Units, Services And Other Products
(8) Money Laundering
(9) Complaints
(10) Media Policy
(11) Miscellaneous

It is the responsibility of each employee to keep abreast with all the Company policies and any ignorance shall not be entertained as a plausible excuse for violating any of the Company policies. Should an employee have any query, require advice, interpretation or any clarification regarding any point such employee(s) are suggested to contact their Head of Department or the Head of HR and Administration department.

All employees are required to sign a code of conduct statement. Such confirmation may include statements that the individual understands the entity's expectations, he/she will always comply with the code of conduct.

c. Creating a Positive Workplace Environment

Without a positive workplace environment, there are more opportunities for poor employee morale, which can affect an employee's attitude about committing fraud against an entity. Factors that detract from a positive work environment and may increase the risk of fraud include following:

• Top management that does not seem to care about or reward appropriate behaviour
• Negative feedback and lack of recognition for job performance
• Perceived inequities in the organization
• Autocratic rather than participative management
• Low organizational loyalty or feelings of ownership
• Unreasonable budget expectations or other financial targets
• Less-than-competitive compensation
• Poor training and promotion opportunities
• Lack of clear organizational responsibilities

Mitigating factors that help create a positive work environment and reduce the risk of fraud includes following:

• Recognition and reward systems that are in tandem with goals and results
• Equal employment opportunities
• Team-oriented, collaborative decision-making policies
• Professionally administered compensation programs
• Professionally administered training programs and an organizational priority of career development

d. Hiring and Promoting Appropriate Employees

The entity will hire qualified individuals, with emphasis on the following;

- educational background,
- prior work experience,
- past accomplishments and
- evidence of integrity and ethical behaviour,

Hiring and promotion procedures may include:

- Conducting background investigations on individuals being considered for employment or for promotion to a position of trust
- Thoroughly checking a candidate's education, employment history, and personal references
- Periodic training of all employees about the entity's values and code of conduct

- Incorporating into regular performance reviews an evaluation of how each individual has contributed to creating an appropriate workplace environment in line with the entity's values and code of conduct

Management needs to clearly articulate that all employees will be held accountable to act within the entity's code of conduct.

7. ANTIFRAUD PROCESSES AND CONTROLS

Neither fraudulent financial reporting nor misappropriation of assets can occur without a perceived opportunity to commit and conceal the act. The management of the company should be proactive in reducing fraud opportunities by

- Identifying and measuring fraud risks (Fraud Risk Assessments)
- **Monitoring Appropriate Internal Controls**
- Identifying Type of Fraud
- Identification of Factors Contributing to Fraud in the Organization
- Implementing Fraud Mitigation Policies

a. Identifying and measuring fraud risks (Fraud Risk Assessment)

The responsibility for establishing and monitoring all aspects of the entity's fraud risk-assessment and prevention activities rest with the management of the company. The management recognisees' that fraud can occur in organizations of any size or type, and that almost any employee may be capable of committing fraud given the right set of circumstances.

In identifying fraud risks, the company take into consideration the organizational and industry characteristics that influence the risk of fraud and complexity of its operations.

The essential elements of an effective fraud risk assessment include:
- A systematic (rather than haphazard) assessment
- Consideration of potential fraud schemes.
- Assessment of risk business unit and significant account levels
- Evaluation of the likelihood and significance of each risk to the company-

Fraud risk-assessment process includes the vulnerability;

- to management override and potential schemes to circumvent existing control activities which may require additional compensating control activities.

- of the company's to fraudulent activity (fraudulent financial reporting, misappropriation of assets, and corruption) and any of those exposures could result in a material misstatement of the financial statements or material loss to the company.

Each department will develope its own operational procedure manual and identifies specific risk involved within the operational procedure of the Department and their mitigates

b. Monitoring Appropriate Internal Controls

Following is the list Control Procedures for monitoring appropriate internal controls

- Ensuring that all transactions are executed in accordance with management's specific authorization in line with delegation of authority document.
- All transactions and other events are promptly recorded in the correct amount, in the appropriate accounts and in proper accounting periods to permit preparation of financial statements are in accordance with an identified financial reporting frame work.
- Ensuring that all reconciliation are properly reviewed and approved by relevant staff
- Ensuring that all sensitive controlling documents have proper approvals
- Checking arithmetical accuracy of records
- Comparing and analyzing the financial results with budget amounts
- Maintaining and reviewing control accounts and trial balance
- Access to assets and records is permitted only in accordance with management authorization.
- Recorded assets are compared with the existing assets at reasonable intervals and appropriate action is taken regarding any difference
- Internal Audit develops an internal audit plan
- Management ensures the implementation of internal audit recommendations
- Controlling applications and environment of computer information system, for example by establishing control over
  - Changes to computer program
  - Access to data files

c. Identification of Type of Fraud

Following Types of Fraud can occur.

i) **Employee Fraud**
Example
• Expense account abuse
• Payroll fraud
• Theft or misappropriation of assets

ii) Computer Crime
Example
• Hacking and other cyber theft

iii) Financial Reporting Fraud

Example

- Asset & revenue misstatement
- Concealed liabilities and expenses
- Improper revenue recognition
- Inadequate omissions or inappropriate disclosures

iv) Medical/Insurance Fraud

Example

- Medical/insurance claims fraud

v) Misconduct and Non-compliance

Example

- Conflicts of interest
- Insider trading
- Non compliance with standard operating procedure (as defined in operating manuals and relevant documents)

vi) Vendor-Related and Other Third-Party Fraud

Example

- Bid rigging and price fixing
- Bribery
- Diversion of sales
- Duplicate billings
- Extortion
- False invoices and ghost vendors
- Inventory theft
- Kickbacks and conflicts of interest

vii) Investor Accounts related Fraud

viii) Settlements and Trade Frauds

Examples of fraud that may be perpetrated are

- Theft, the appropriation or misuse of assets for personnel benefit;
- Bribery and corruption – offering, giving, soliciting or acceptation an inducement or reward that may influence the action taken by the office or its staff, for example in procurement of goods and services
- False accounting and / or making fraudulent statements with a view to personnel gain for another, for example falsely claiming overtime, travel and subsistence, sick leave or special leave (with or without pay); and
- Externally perpetrated fraud against the company, for example in procurement and delivery of goods and services
- Late Trading in Funds Units after official timing to profit from market events.

- Creating or and making transaction on the basis Ghost Unit Holder(s)

- Insider or Personnel Trading against company's Personal Share Dealing Policy as defined in code of conduct and ethics policy

d. Identification of Factors Contributing to Fraud in the Organization

Following factors may contribute chances of fraud in the Organization

- Collusion between Employees and Third Parties
- Inadequate Internal Controls
- Management Override of Internal Controls
- Collusion between Employees and Management
- Lack of Control over Management by Directors
- Ineffective or Non existent Ethics or Compliance Program

e. Identifying Steps to Mitigate Risks

Following are the risk mitigating steps:

- Reviewed or Strengthened Internal Controls
- Instituted Periodic Internal Audits
- Ensuring that all transactions or events are conducted in line with delegation of authority / expenditure approval procedure and guidelines document as approved by the board
- Created an Employee Hotline
- Appointed Compliance Personnel
- Establish a Code of Conduct for All Employees
- Conducted Background Checks for New Employees
- Instituted Fraud Awareness Training
- Tied Employee Evaluations to Ethics or Compliance Objective

8. APPROPRIATE OVERSIGHT PROCESS

Oversight can take many forms and can be performed by many within and outside the entity including:

- Audit Committee and Board
- Management
- Internal Auditors
- External Auditors

a. Audit Committee or Board of Directors

The board, in its fiduciary role, is responsible for overseeing the internal controls over financial reporting established by management and the process by which management satisfies itself that they are working effectively. The board is also responsible for assessing the risk of financial fraud by management and ensuring controls are in place to prevent, deter and detect fraud by management.

The audit committee plays an important role in its oversight responsibilities with respect to the entity's financial reporting process and the system of internal control. The audit committee Oversight includes:

- Evaluation of management's activities relating to process for identifying and documenting fraud risk
- Ensure that senior management implements appropriate fraud deterrence and prevention measures to better protect stakeholders.
- Obtain from the internal auditors and independent auditors their views on management's involvement in the financial reporting process.
- Assess the strength of the company internal control and the potential for fraudulent financial reporting using information received in communications from the independent auditors.

b. Management

The primary responsibility for the prevention and detection of fraud and error rest with both those charged with the governance and the management of the company. It is the responsibility of the management of an entity to establish a control environment and maintain policies and procedure to assist is achieving the objective of ensuring as far as possible, the orderly and efficient conduct of entity's business. Management with the oversight of those charged with governance, need to set proper tone, create and maintain culture of honesty and high ethics, and establish appropriate controls to prevent and detect fraud and error within the company

The management should ensure integrity of the company's accounting and financial reporting system and appropriate controls are in place, including those monitoring risk, financial control and compliance with relevant laws

c. Internal Auditors

An effective internal audit can be extremely helpful in performing aspects of the oversight function. Their knowledge about the company may enable them to identify indicators that suggest fraud has been committed.

Internal auditors should assist in the deterrence of fraud by identifying indicators of fraud and fraud risks, examining and evaluating the adequacy and the effectiveness of the system of internal controls, and recommending action to mitigate risks and improve controls.

Internal auditors, in carrying out this responsibility, should determine if the Company has an environment that fosters control consciousness, realistic goals and objectives, written policies that describe prohibited activities and the action required whenever violations are discovered. They should also determine if company has:

- Established and maintains appropriate authorization policies for transactions
- Developed policies, practices, procedures, reports, and other mechanisms to monitor activities and safeguard assets
- Developed communication channels that provide adequate and reliable information

Internal auditors should have an independent reporting line directly to the audit committee, to enable them to express any concerns about management's commitment to appropriate internal controls or to report suspicions or allegations of fraud involving management.

d. External Auditor

It is not the external auditor's function to prevent fraud and irregularities, but external auditor has a responsibility to review the company's internal controls for preventing and detecting fraud and error.

External auditors should provide the audit committee with an assessment of the Company's process for identifying, assessing, and responding to the risks of fraud. External auditors if consider necessary should highlight management's risk assessment process, the system of internal control, the company's susceptibility to fraudulent financial reporting, and the entity's exposure to misappropriation of assets to Audit Committee and Board of Directors

9. FRAUD RESPONSE PLAN

This fraud response plan provides a checklist of actions and a guideline to follow in the event that fraud is suspected. It defines authority levels, responsibilities for action and reporting lines in the event of suspected fraud, theft or other irregularity. Fraud Response Plan covers following:

- Notifying suspected fraud;
- The investigation process;
- Liaison with police and external audit;
- Initiation of recovery action;
- Reporting process;
- Communication to Audit Committee

a. Notifying Suspected Fraud

It is important that all staff are able to report their concerns without fear of reprisal or victimisation and are aware of the means to do so. In the first instance, the staff should report any suspicion of fraud, theft or other irregularity, as a matter of urgency, to its senior(s). If such action would be inappropriate, staff concerns should be reported upwards to one of the following persons:

- Head of Department (or equivalent);
- Head of Compliance;
- Chief Financial Officer
- Chief Executive.

Every effort will be made to protect an informant's anonymity if requested. However, the company will always encourage individuals to be identified to add more validity to the accusations and allow further investigations to be more effective. In certain circumstances, anonymity cannot be maintained. This will be advised to the informant prior to release of information.

b. The Investigation Process

Suspected fraud must be investigated in an independent, open-minded and professional manner with the aim of protecting the interests of both the company and the suspected individual(s). Suspicion must not be seen as guilt to be proven.

The investigation process will vary according to the circumstances of each case and will be determined by the Chief Executive in consultation with Chief Financial Officer, Head of Compliance and Head of Relevant Department. An "Investigating Officer" will be appointed to take charge of the investigation on a day-to-day basis. This will normally be the Head of Compliance or, exceptionally, another independent Head.

The Investigating Officer will appoint an investigating team. This will normally comprise staff from within the Compliance and Risk Management Department but may be supplemented with other resources from within the company or from outside.

Where initial investigations reveal that there are reasonable grounds for suspicion, and to facilitate the ongoing investigation, it may be appropriate to suspend an employee against whom an accusation has been made. This decision will be taken by the Chief Executive in consultation with the Head of Human Resources and the Investigating Officer. Suspension should not be regarded as disciplinary action nor should it imply guilt.

It is important, from the outset, to ensure that evidence is not contaminated, lost or destroyed. The investigating team will therefore take immediate steps to secure physical assets, including computers and any records thereon, and all other potentially evidential documents. They will also ensure, in consultation with management, that appropriate controls are introduced to prevent further loss.

The Investigating Officer will ensure that a detailed record of the investigation is maintained. This should include a chronological file recording details of all telephone conversations, discussions, meetings and interviews (with whom, who else was present and who said what), details of documents reviewed, tests and analyses undertaken, the results and their significance. Everything should be recorded, irrespective of the apparent significance at the time.

All interviews will be conducted in a fair and proper manner. Where there is a possibility of subsequent criminal action, the police will be consulted and interviews may be conducted under caution in compliance with the relevant laws, which governs the admissibility of evidence in criminal proceedings.

The findings of the investigation will be reported to the Chief Executive and Chief Financial Officer, who will determine, in consultation with the Investigating Officer, what further action (if any) should be taken.

c. Liaison with Police & External Audit

The Chief Executive, following consultation with the Chief Financial Officer, Head of Compliance and the Investigating Officer will decide if and when to contact the police.

The Chief Financial Officer will report suspected frauds to the external auditors at an appropriate time.

All staff will co-operate fully with any police or external audit enquiries, which may have to take precedence over any internal investigation or disciplinary process. However, wherever possible,

teams will co-ordinate their enquiries to maximise the effective and efficient use of resources and information.

d. Initiation of Recovery Action

The company will take appropriate steps, including legal action if necessary, to recover any losses arising from fraud, theft or misconduct. This may include action against third parties involved in the fraud or whose negligent actions contributed to the fraud.

e. Reporting process

Throughout any investigation, the Investigating Officer will keep the Chief Executive, informed of progress and any developments. These reports may be verbal or in writing. On completion of the investigation, the Investigating Officer will prepare a full written report setting out:

- Background as to how the investigation arose;
- What action was taken in response to the allegations;
- The conduct of the investigation;
- The facts that came to light and the evidence in support;
- Action taken against any party where the allegations were proved;
- Action taken to recover any losses;
- Recommendations and/or action taken by management to reduce further exposure and to minimise any recurrence.

In order to provide a deterrent to other staff a brief summary of the circumstances will be circulated to all the staff.

f. Communication to Audit Committee

Irrespective of the amount involved, the all cases of attempted, suspected or proven fraud shall be reported to Audit Committee. The Head of Compliance is responsible for preparation and submission of fraud reports to Audit Committee.