VESTLAND BERHAD

ANTI-FRAUD AND WHISTLEBLOWING POLICY

1.0 ANTI-FRAUD POLICY

1.1 DEFINE FRAUD

Fraud refers to any deceptive act with the intention of seeking personal interests, circumventing obligations or causing losses in collusion with business partners.

Examples of fraudulent behaviors include:

- misstatement on one's expenses.
- kickback (including undue gifts or cash accepted).
- offering or accepting bribery.
- unauthorised pricing.
- fictitious suppliers.
- embezzlement of assets (including cash) in one's position
- fraudulent financial statements.
- fraud relating to cheque and salary.
- fraud relating to occupation (abusing or misusing the employer's resources or assets to line one's own pocket by taking advantage of one's duty).

1.2 FRAUD RISK FACTORS

Fraud risk factors are events and conditions that increase the likelihood of occurrence of fraud. Such factors include:

(a) the rationalisations or attitudes to justify a fraudulent action.
(b) the incentives or pressures to perpetrate fraud.
(c) the opportunity to commit fraud.

The following examples of events or conditions indicate high fraud risks in a business:

(a) Internal Control
- inadequate or ineffective internal control and slow improvement.
- use of brokers with indefinite arrangement or inappropriate business mix
- absence of timely and correct transaction records
- significant, exceptional and/or complex transactions.

(b) Assets
- slack physical control of fixed assets, cash and cash equivalents.
- inadequate monitoring of travel, entertainment and gift expenses.
- improper asset records.
- required material measurement and evaluation of assets.

(c) IT System
- absence of robust access control.
- absence of access control for the human resources system and the financial reporting system.
- improper authorisation system and transaction approval.
- misconduct of the employees due to vulnerable security.

(d) Business Environment
- advancement of science and technology.
- increasing complexity of organisation setup.
- an increasing number of contract or temporary workers.
- economic recession.

1.3 ANTI-FRAUD

Vestland Group has zero-tolerance to fraud and requires all employees to always act honesty and with integrity and to safeguard the assets for which they are responsible.

The Group shall be responsible for:
- setting code of conduct and the culture of good faith.
- advocating high ethical standards and professionalism.
- developing effective internal controls to prevent fraud.
- carrying out vigorous investigations if fraud occurs.
- taking appropriate disciplinary and/or legal action against fraudsters.

Management shall be responsible for:
- identifying the risks to which systems and procedures are exposed.
- developing effective internal controls to prevent and detect fraud.
- ensuring key controls are being complied with.
- encouraging employees to be vigilant and raising fraud-awareness at all levels.

Employees shall be responsible for:
- acting with propriety in the handling and use of assets.
- complying with the policies and controls set.
- being alert to unusual events or transactions which could possibly be indicators of fraud.
- reporting immediately to superior if they aware of any suspicious activities.

1.4 ANTI-FRAUD MEASURES

Anti-fraud measures shall be put in place to decrease motive, restrict opportunity and limit the ability for potential fraudsters to rationalize their actions. Anti-fraud measures include:

(a) sound ethical culture and environment – guiding philosophy drawn up by top management and good ethical examples demonstrated by top management
(b) periodic assessment of fraud risk – periodically identify fraud risks within organisation at all levels and assess the impact and likelihood of fraud risks identified.
(c) Code of Conduct in place and ethics training – to raise awareness through formal education (formal training, group meetings, internal memos etc) and ongoing communication within organisation.
(d) sound internal control system – key controls shall be put in place over organisation's systems and processes to support its effective and efficient operation.
(e) pre-employment screening – the process of verifying the background, qualification, suitability and experience of a potential employment.
(f) whistleblowing – establish an effective reporting mechanism for fraud to encourage employee to speak out and report any suspicious actions.

1.5 TREATMENT OF SUSPECTED FRAUD

Suspected fraudulent behaviors shall be addressed as follows:

(a) All information received is considered highly confidential.
(b) Suspected misconduct or delinquency must be investigated into with discretion, so as not to give rise to exposure, or framing, or let the suspects know an investigation is going on.
(c) No manager or employee is allowed to initiate a fraud investigation until the Board of Directors confirms and reaches agreement on the investigation process.
(d) When a suspected fraud is discovered, the competent manager must assure security of relevant information (photocopies or electronic files) from the outset and provide files for investigation and subsequent procedures.

The reasonable steps for responding to suspected fraud include:

(a) clear reporting mechanism – the procedures for reporting fraud are spelt out clearly in a formal whistleblowing policy.
(b) thorough investigation – an investigation team to be established to formulate a response (scope, resources, timeline, action plan, outcome).
(c) disciplinary actions over individuals responsible – include internal disciplinary action, civil response, criminal prosecution or both.
(d) recovery of stolen assets or funds, if applicable.

1.6 THE GOLDEN RULE OF FRAUD REPORTING

(a) All evidence must be well protected and the Board of Directors must be informed of.
(b) Never tangle with the employee in question, or do investigation without permission, or tell anybody else your doubts.

1.7 IDENTIFY FRAUD

It is assumed that anyone could commit a fraud when the conditions are right. It is important to use your knowledge of internal controls to spot loopholes and prove your suspicions.

Keep firmly in mind that proper paperwork is not equivalent to the truth. Perhaps, someone is trying in vain to cover up the truth. Pay attention to written documents and the attachments and check if the dates, figures, amounts, taxes and other clauses therein are consistent and logical. Look into the account balances and accounting vouchers and particularly pay attention to adjustments.

2.0 WHISTLEBLOWING POLICY

2.1 OVERVIEW

The Group is committed to the highest possible level of transparency, integrity and accountability. Hence, the Group expects and encourages all employees to call attention to any alleged misconduct or delinquency occurring in the Group.

This whistleblowing policy is intended to:

(a) provide a platform allowing the employees to report any misconduct or delinquency that exist in the Group.
(b) prohibit retaliation against employees raising such misconduct or delinquency.
(c) establish procedures for responding to any reports from employees regarding such misconduct or delinquency.

For this policy, a person who exposes misconduct or delinquency is called a whistleblower.

The Group will try the best to respond to any employee's concerns in a fair and appropriate manner, though the Group may not always be able to address a reported event in the way desired by the whistleblower.

2.2 WHISTLEBLOWER PROTECTION AND SUPPORT

A whistleblower who lodges a complaint based on the policy can rest assured that he/she will not be terminated, face retaliation or suffer unnecessary disciplinary punishments even if his/her concerns are not supported by concrete evidence in the end, provided that the whistleblowing is done in good faith.

Where the whistleblower lodges a complaint based on the policy for the purpose of doing harm to or taking revenge on somebody else, he/she will receive counseling and/or face disciplinary action and might be dismissed based on the severity of the complaint.

2.3 RESPONSIBILITIES OF POLICY IMPLEMENTATION

The policy will be implemented at the discretion of the Board of Directors and the Audit and Risk Management Committee. The Board of Directors and the Audit and Risk Management Committee shall have the overall responsibility to monitor and review the implementation of the policy and to advise on investigations into complaints.

The management must make sure all employees have no inhibitions about raising their concerns. All employees must make sure that they take appropriate actions to disclose any misconduct or delinquency they become aware of. Where any employee has any doubts over the content or application of the policy, he/she should contact the Human Resources Department.

When an investigation is launched, the Group must understand the utmost importance to assure and maintain the confidentiality of all persons involved in the investigation. They must make a statement to declare free of conflicts of interest before the investigation starts. Where a conflict of interest is found at any stage, the persons concerned must be replaced immediately.

2.4 MISCONDUCT OR DELINQUENCY

It is impossible to produce an exhaustive list of misconducts or delinquencies, but, the Group expects the employees to report:

(a) Criminal offences or illegal activities;
(b) Default on any legal obligation;
(c) Injustice;
(d) Malpractice or fraud in relation to accounting, financial reporting, auditing, internal control and other financial matters;
(e) Theft of cash, properties or any other assets;
(f) Fraudulent reimbursement requests;
(g) Fraudulent activities plotted in collusion with partners, suppliers or competitors, such as bribery, illegal gratuities, economic extortion, concealment of conflicts of interest and abuse of power;
(h) Other financial malpractices;
(i) Unauthorised use or disclosure of business intelligence;
(j) Breach of the Company's rules and regulations;
(k) Improper conduct or immoral act;
(l) Any act jeopardizing the health or safety of any person;
(m) Any act harmful to the environment; and
(n) Intentional concealment of data related to the aforesaid matters.

Although it is not mandatory, however it is advisable for the whistleblower to provide absolute evidence proving the misconduct or delinquency he/she reports, but his/her concerns must be well grounded.

2.5 FALSE WHISTLEBLOWING

Where the whistleblower has a hidden agenda or cannot justify the truthfulness or reliability of the concern reported, or makes a false allegation out of malice, grudge or revenge, he/she might be subject to disciplinary actions, which may result in termination.

2.6 WHISTLEBLOWING METHOD

When a whistleblower is of the opinion that there is any suspected misconducts, he/she shall make a report in writing to the Board of Directors and the Audit and Risk Management Committee through the Whistleblowing Email.

The Whistleblowing Email is a confidential mailing service which offers employees the possibility to report to the Board of Directors and the Audit and Risk Management Committee any concerns in confidence without any party in Vestland Group knowing about the disclosure initially. The Whistleblowing Email is **whistleblowing@vestland.com.my** and hotline at **+6017 8899326**

The whistleblower is required to report any suspected misconducts in good faith immediately, providing as much information as possible including:

(a) The name and contact details of whistleblower
(b) The details on the concerns (background, nature of wrongdoings, reasons for concern)
(c) The name of the person in question
(d) The time and place of occurrence
(e) The details of witness and factual corroborating evidence, if any,
(f) The particulars of documentary evidence, if any.

The whistleblower is required to disclose his/her name and contact details. However, the whistleblower may choose to remain as anonymous.

2.7 PRIVACY

The Group will protect the privacy of the whistleblower to the fullest extent possible and in accordance with applicable laws.

Whistleblower shall keep the nature of his/her concerns and the persons involved in strict confidential to avoid retaliation or mistreatment.

Under some circumstances, the nature of investigation may necessitate public disclosure of the whistleblower's identity. However, the identity and particulars of whistleblower will not be disclosed without prior consent of the whistleblowing unless required by law.

Likewise, if the investigation leads to criminal proceedings, the whistleblower might be asked to provide evidence and a written statement or talk with the relevant authorities face to face. Under this circumstance, the Group will try the best to keep the identities of the whistleblower confidential.

However, the whistleblower should understand that under some circumstances, the Group might need to refer the cases to the relevant authorities without prior notice or consultation.

2.8 INVESTIGATION PROCEDURE

(a) Upon receiving of the report, the Audit and Risk Management Committee will decide if a thorough investigation is necessary.

(b) The Audit and Risk Management Committee will seek legal advice if the report exposes alleged criminal offences and decide whether to refer the case to the relevant authorities for next steps.

(c) If the case is referred to the relevant authority, the Audit and Risk Management Committee will be unable to proceed with their own investigation.

(d) The appointment of the investigation team will be made by the Audit and Risk Management Committee if a thorough investigation is necessary.

(e) The whistleblower might be requested to produce more evidence for the investigation. The whistleblower is expected to give full cooperation throughout the investigation process.

(f) The investigation team shall submit an update or written report to the Audit and Risk Management Committee after investigation. The Audit and Risk Management Committee shall have the final decision on the disciplinary actions to be taken, if applicable.

(g) Possible investigation results:
   (i) The allegation cannot be corroborated; or
   (ii) The allegation is corroborated, and either one or both actions will be taken:
      - Make corrections and promise such a problem will never occur again; and
      - Take disciplinary or appropriate actions against the violators.

2.9 SUPERVISORY POLICY

The Board of Directors and the Audit and Risk Management Committee will preserve all records of complaints, including date of complaint, investigation summary, result, advice for improvement and actions taken.

The Board of Directors and the Audit and Risk Management Committee will supervise and review the implementation and effectiveness of the policy on a regular basis.