



NESTCON GROUP

BUILDING INTEGRITY . CONNECTING COMMUNITIES

**ANTI FRAUD AND
WHISTLEBLOWING POLICY**

TABLE OF CONTENTS

1.0 ANTI FRAUD POLICY		
1.1	DEFINE FRAUD	3
1.2	FRAUD RISK FACTORS	3
1.3	ANTI FRAUD	3
1.4	ANTI FRAUD MEASURES	4
1.5	TREATMENT OF SUSPECTED FRAUD	4
1.6	THE GOLDEN RULE OF FRAUD REPORTING	4
1.7	IDENTIFY FRAUD	4
2.0 WHISTLEBLOWING POLICY		
2.1	OVERVIEW	5
2.2	WHISTLEBLOWER PROTECTION AND SUPPORT	5
2.3	RESPONSIBILITIES FOR POLICY IMPLEMENTATION	5
2.4	MISCONDUCT OR DELINQUENCY	5
2.5	FALSE WHISTLEBLOWING	6
2.6	WHISTLEBLOWING METHOD	6
2.7	PRIVACY	6
2.8	INVESTIGATION PROCEDURE	7
2.9	SUPERVISORY POLICY	8

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. In the Company, fraudulent behaviors include: misstatement on one's expenses; kickback (including undue gifts or cash accepted); offering or accepting bribery; unauthorized pricing; fictitious suppliers; embezzlement of the Company's assets in one's position; fraudulent financial statements; the risk of existing or potential financial loss arising out of conflicts of interest; and fraud relating to cheque, salary and occupation. Fraud relating to occupation is defined as an act of 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 include employees, internal control, assets and IT:

- (a) Employees: turnover of senior management or the staff; improper screening of candidates; absence of a rotation mechanism for key functions; management and the staff overstressed by performance targets.
- (b) 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.
- (c) 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, liabilities, revenue or expenses.
- (d) IT: absence of robust access control for the IT system; absence of access control for the human resources system and the financial reporting system; improper authorization system and transaction approval; misconduct of the employees due to vulnerable security of the IT system.

In the present economic environment, fraud is more prone to occur because of the following reasons: advancement of science and technology; increasing complexity of organization setup; an increasing number of temporary workers; and economic recession.

1.3 ANTI FRAUD

We seek to improve the process and nip fraud in the bud by adhering to a set of code of conduct and the culture of good faith, high ethical standards and professionalism, and knitting effective internal control into the fraud risk evaluation process.

The Board of Directors organizes a formal fraud risk evaluation on an annual basis. Key fraud risks are evaluated and recorded. The controls intended to avoid the fraud risks identified are examined and optimized. The Human Resources and Administration Department will arrange for trainings on professional ethics and fraudulent behaviors. All managers must evaluate fraud risks within their scope of duty constantly and make sure adequate controls are in place. Material fraud risks must be reported to the Board of Directors.

1.4 ANTI FRAUD MEASURES

Anti-fraud measures are detailed as follows: guiding philosophy drawn up by the top management; good leadership; rotation of the staff; background check of new recruits; compliance with the Code of Conduct; assessment of the employees against ethical or compliance standards; ethics training.

1.5 TREATMENT OF SUSPECTED FRAUD

Suspected fraudulent behaviors are addressed as follows. All information received is considered highly confidential. 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. No manager or employee is allowed to initiate a fraud investigation until the Board of Directors confirms and reaches agreement on the investigation process. 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.

1.6 THE GOLDEN RULE OF FRAUD REPORTING

First of all, all evidences must be well protected and the Board of Directors must be informed of. 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 fabulous paperwork is not equivalent to the truth. Perhaps, someone is trying in vain to cook 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 policy is intended to provide a mechanism allowing the employees to report any malpractice existing in the Group to the Audit Committee under the condition of confidentiality and map out the investigation procedure.

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. For the purpose of 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 or she will not be fired, or mistreated for no reason or suffer unnecessary disciplinary punishments even if his or her concerns are not supported by concrete evidences in the end.

Where the whistleblower lodges a complaint based on the policy for the purpose of doing harm to or taking revenge on somebody else, he or she will be punished and might even be dismissed.

2.3 RESPONSIBILITIES OF POLICY IMPLEMENTATION

The policy will be implemented at the discretion of the Board of Directors and the Audit Committee. The Board of Directors and the Audit Committee have the 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 or she should contact the Board of Directors.

When an investigation into any matter reported by the whistleblower is launched, the Group must understand the utmost importance to assure and maintain independence of all persons involved in the investigation. They must make a statement on their personal interests 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 generally speaking, 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) Unauthorized 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.

The Group does not expect the whistleblower to provide absolute evidence proving the misconduct or delinquency he or she reports, but his or her concerns must be well grounded.

The whistleblower deserves respect and appreciation for his or her effort out of goodwill, even if the Group does not launch an investigation.

2.5 FALSE WHISTLEBLOWING

Where the whistleblower has a hidden agenda, or cannot justify the truthfulness or reliability of the thing reported, or makes a false whistle-blowing out of malice for the sake of personal interests, he or she might be subject to disciplinary actions or be dismissed.

2.6 WHISTLEBLOWING METHOD

The whistleblower is required to file a written report. The report must bear the whistleblower's signature and be enclosed in an envelope. The envelope is marked as In Strictly Confidential on its cover and submitted to the Board of Directors or the Audit Committee. Alternatively, the report can be e-mailed to anti-fraud@nestcon.my (Attention to Independent Non-Executive Audit Committee Chairman) addressed to the Board of Directors and the Audit Committee.

The whistleblower is expected to provide complete data in the report, inclusive of but not limited to:

- (a) Name and contact information of the whistleblower, including phone number, email address and address; and
- (b) Details on the concerns: name of the person in question, date of report, place and reasons, and evidence (if any).

We respect that sometimes you may wish to file the report in confidential. However, an anonymous allegation will be much more difficult for the Company to follow up simply because we will not be able to obtain further information from you and make a proper assessment.

Although anonymous reporting is not prohibited, we generally do not encourage anonymous reporting and encourage you to come forward with your concerns.

2.7 PRIVACY

The Group shall do the best to protect privacy of the whistleblower. To avoid negative influence on the investigation, the whistleblower shall also keep the nature of his or her complaints or concerns and the persons involved in strictly confidential.

Under some circumstances, the nature of investigation may necessitate public disclosure of the whistleblower's identity. In that case, the Group shall do the best to inform the whistleblower of the possibility of disclosure of his or her identity. If the whistleblower needs to get involved in the investigation, his or her identity as the whistleblower will be kept confidential where possible. But it is also possible that his or her identity as the whistleblower might be found out by a third party during the investigation.

Likewise, if the investigation leads to criminal proceedings, the whistleblower might be asked to provide evidences or talk with the competent authorities face to face. Under this circumstance, the Group will try the best to discuss the influence on privacy with the whistleblower.

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

2.8 INVESTIGATION PROCEDURE

- (a) The Group will reply to the whistleblower within seven working days after a report is received therefrom, to acknowledge:
 - (i) Receipt of the report;
 - (ii) Serious consideration to be made; and
 - (iii) The promise to inform the whistleblower of the investigation result as soon as possible to the extent permitted by law.
- (b) The Group will decide whether a thorough investigation is necessary after receiving a report.
- (c) When a report exposes alleged criminal offences, the Group will consult the legal advisor, and decide whether to refer the case to the competent authorities for next steps.
- (d) Most of the time, the Group will do the best to discuss with the whistleblower before referring a case to the competent authorities, but in some cases, the Group might need to refer a case to the competent authorities before informing or consulting the whistleblower.
- (e) Once a case is referred to the competent authorities, the Group is unable to take any step in relation to the case, including informing the whistleblower.
- (f) The whistleblower might be requested to make available more evidences during the investigation.
- (g) Possible investigation results:
 - (i) The allegation cannot be corroborated; or
 - (ii) The allegation is corroborated, and either one or both of these two actions will be taken:
 - ❖ Make corrections and promise such a problem will never occur again; and
 - ❖ Take disciplinary or appropriate actions against the violators.
- (h) The whistleblower will be informed of the investigation result in a written form. To the extent permitted by law, the Group might be unable to provide details on the actions taken or a copy of the report to the whistleblower.
- (i) If the whistleblower is unsatisfied with the investigation result, he or she may lodge a complaint with the Board of Directors and the Audit Committee again. The whistleblower needs to prepare another report to explain why he or she is unsatisfied. The Group will launch another investigation only with good reason.

- (j) At this stage, of course, the whistleblower may lodge his or her concerns with the competent authorities such as the regulator or the law enforcement agency. Nevertheless, they must have sufficient evidences to support their concerns. The Group encourages them to discuss with the Board of Directors and the Audit Committee before disclosing the matters to the public.
- (k) The whistleblower may also consult his or her legal advisor.

2.9 SUPERVISORY POLICY

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