



"HATCHING FOR THE FUTURE"

TEO SENG GROUP OF COMPANIES

ANTI-CORRUPTION POLICY

TABLE OF CONTENTS

1	SCOPE AND OBJECTIVES	1
2	APPLICABILITY	2
3	POLICIES AND PRINCIPLES	2
4	RISK-BASED APPROACH.....	5
5	RECOGNITION & REPORTING OF SUSPICIOUS CORRUPTION AND UNETHICAL ACTIVITY.....	6
6	COMMUNICATION, AWARENESS & TRAINING	7
7	RECORD KEEPING AND INFORMATION SHARING	8

DOCUMENT VERSION

Month & Year	Version	Prepared By	Comment Change
Apr 2020	1.0	Gan Han Long	First drafted framework

REFERENCES & APPENDIXES

Appendix 1.0	Enterprise Risk Management and Sustainability Governance

1 SCOPE AND OBJECTIVES

Teo Seng Capital Berhad and its subsidiaries' ("the Group") core value in conducting business and dealing with its stakeholders is integrity. In order to practice and achieve the Group's core value, the Group believes that a sound and proper system shall be put in place and shall be maintained and updated from time to time. To gain trust and confidence from the stakeholders will definitely help to reflect the integrity value practiced by the Group. To prevent any breach in the integrity of the Group which will result in jeopardising the business of the Group, hence stakeholders losing confidence in the Group, the system employed by the Group shall be robust and always in compliance with the relevant laws and regulations that will prevent the Group from being used by unscrupulous individuals or entities to commit harm or losses to not only innocent customers, but also to the government, society and the world at large.

In this regard, processes are emplaced to prevent the Group's products, services or channels from being used for unethical or illegal activities as well as safe-guarding information and data. Control measures are also being emplaced to identify, assess, mitigate, monitor and report such risks as similarly adopted process in ERM framework. They include conducting due diligence on all staff, including the board of directors, customers, vendors and third parties before the Group accepts and on-boards the relationship as well as ensuring all staff understand their obligations through effective training and awareness programmes.

The Group demonstrates its full commitment and support to high standards of compliance with the relevant requirements by establishing a comprehensive policy, procedures, processes and systems for the prevention and detection of bribery activities. This Anti-Corruption Policy ("the Policy") set out the standards of responsibility and obligations of the Group's employees (including Board of Directors) to assure fair dealing, integrity and ethical conduct, workplace safety and harmony, safeguard of confidential information as well as prevent conflict of interest with the Group. The Policy outline general principles serve as our guide to moral and ethical behaviour that is expected from all employees, it does not cover every issue that may arise out of the Policy. Employees are expected to always uphold integrity and exercise due care in all dealing to act ethically and in the interest of the Group.

2 APPLICABILITY

The Policy is applicable to all employees (including full time, probationary, contract and temporary staff) of the Group. This Policy shall form an integral part of the terms and conditions of employment in which every employee is obligated to understand and adhere to the Policy. Non-compliance of the Policy by any employee will be treated severely with disciplinary action, including termination of employment.

3 POLICIES AND PRINCIPLES

3.1 Compliance with Laws, Rules and Regulations

- 3.1.1 Employees shall comply with all laws, rules and regulations and guidelines applicable to the Group's operation when performing their duties. Attention shall also be given to general public order and industrial best practices.
- 3.1.2 Employees have responsibility to be sufficiently familiar with legislation or regulations that relevant to their scope of duties and to recognise potential liabilities, when uncertain about the application or interpretation of any legal requirements should refer the matter to their superior, if necessary, seek appropriate legal advice.
- 3.1.3 Employees must not engage in or give the appearance of being engaged in any illegal or improper conduct that is in violation of this Policy or that indicates a casual attitude toward compliance with laws, regulations or this Policy.

3.2 Conflict of Interest

- 3.2.1 Employee shall act in good faith and bona fide in the interest of the Group, with reasonable effort to avoid business, financial or other direct or indirect interests or relationships which conflict with the interests of the Group, or which divides his/her loyalty to the Group.
- 3.2.2 All activities conducted as an employee of the Group should always place the lawful and legitimate interests of the Group over personal gain.
- 3.2.3 When facing situation that may involve or lead to a conflict of interest, the employee shall disclose it to his/her Line Manager and/or the HR and resolve in a fair and transparent manner.
- 3.2.4 Employee should notify his/her manager in writing immediately upon becoming aware of a conflict, whether real or perceived, either involving him/herself, another employee or a third party.
- 3.2.5 Employment of employee's family members and relatives may be allowed subject to proper declaration made prior to acceptance of employment and that may subject to conditions determined by the Group.

- 3.2.6 No employee shall use his or her position with the Group or information acquired during employment in a manner that may create a conflict, or the appearance of a conflict, between the employee's personal interests (included but not limited to their families, or any other person) and those of the Group.
- 3.2.7 No employee shall involve or participate in any discussion and decision which may result of improper personal benefit gains.
- 3.2.8 No employee shall induce or collaborate with others to enter any business dealings or transactions to gain his/her personal interests.

3.3 Dealing in Securities / Insider Trading or Dealing

- 3.3.1 Insider trading is strictly prohibited by the Group and it is an offence defined under the Capital Markets and Services Act 2007 which is liable to legal proceeding; thus employees must not trade in the Group's shares or securities on the basis of material non-public price sensitive information or during closed period of announcements to Bursa Securities if any.
- 3.3.2 Employees shall not disclose to anyone inside or outside the Group any material non-public information obtained in the course of performing their duties and responsibility unless it is authorised or legally mandated.
- 3.3.3 Employees shall not derive profit or assist others to gain profit on trading the Group's securities from any confidential information or non-disclosure of sensitive information.
- 3.3.4 Employees must consult their respective Line Manager or the Group Secretary for any uncertainty as to the nature of information in their possession in relation to materiality and/or price sensitivity.

3.4 Privacy & Confidentiality of Information

- 3.4.1 Employees shall exercise due care and diligence in performing their duties to maintain strictest confidential information concerning the Group's business, its customers, suppliers, trade secrets and any proprietary information to which the employees have access or possessed by the employees.
- 3.4.2 Employees' obligation to maintain confidentiality of Group's information shall continue to apply after termination of employment.
- 3.4.3 Employees shall ensure that a proper non-disclosure or confidentiality agreement is concluded with third parties in advance if the disclosure of trade secret to such third parties is required in the course of business transaction.
- 3.4.4 Employees shall refrain from discussing confidential Group businesses with outsider or any other third person who should not have a legitimate need to know the information.
- 3.4.5 Employees shall respect and take all necessary measures to preserve intellectual property rights ("IP") which include patent, trademarks, copyrights and trade secrets of the Group and that of other Group. Employees' act of infringing IP owned by the Group or by other

Group will not be tolerated e.g. unauthorised copying of computer software or imitated trademark of other Group.

3.5 Gifts & Hospitality

- 3.5.1 Employees shall not solicit or receive/give a valuable gift or favor from/to any person, Group, organisation, or intermediary that will directly or indirectly lead to the occurrence of potential conflict of interest. In other words, gift or hospitality that considered will impair effective judgement, improper influence a decision or reaction is highly prohibited.
- 3.5.2 Employees may accept unsolicited meal, refreshment or entertainment on an occasional basis if such courtesies are not lavish or extravagant and acceptance will promote good business relation, or with approval from the Management on the ground that the value involved is not significant and clearly will not create an obligation to the donor.
- 3.5.3 Employees shall not receive or offer, directly or indirectly, any valuable gifts, remuneration, hospitality, donations, illegal payments and comparable benefits which shall include but not limited to cash, preferred loan, security or secret commission.
- 3.5.4 The best practice is usually to accept the gift on behalf of the Group, report it to respective Line Manager and turn the gift over to the Group to prevent against any undue obligations of the employee to any outside parties.

3.6 Working Attitude

- 3.6.1 Employees should always deal fairly and honestly regardless with customers, suppliers or any other third party whom has business relation with the Group.
- 3.6.2 Employees shall not engage in fraudulent or any other dishonest conduct involving the property or assets or the financial reporting and accounting of the Group or any third party.
- 3.6.3 Employees shall protect Group's assets against waste, loss, damage, misuse, theft, misappropriation or infringement and for using those assets in responsible ways.

4 RISK-BASED APPROACH

A risk-based approach should be adopted to ensure that measures to prevent or mitigate corruption and unethical activity are commensurate with the risks identified and that effort is directed proportionately with appropriate flexibility to effectively manage areas with real risks. The GROUP has summarised a risk-based approach as covering:

- Risk-identification and assessment
- Risk mitigation
- Risk monitoring
- Documentation

Reasonable steps must be taken to identify and strengthen any weak links in the internal controls and processes with proportionate time and recourse focused on strengthening the weak links. The management of the GROUP has been tasked to ensure that risks are managed appropriately.

Risk-identification and assessment

The risk assessment process is to identify and determine the inherent risks i.e. before any controls being applied, on corruption and unethical activity that the business is exposed to, thus allowing the design of appropriate mitigating controls and strategy.

The risk assessment is not a one-off process but a continual effort. The GROUP must assess the different types of inherent risks regularly, as well as when changed circumstances arise. Any risk identified during the assessment shall be highlighted and additional controls or assurance work identified can be incorporated.

Risk mitigation

Controls must be designed and implemented to mitigate the inherent risks identified. It is understood that no control can completely eliminate the risks therefore the residual risks need to be assessed in order for the GROUP to determine if they are content with the risk exposure or to implement additional controls to further mitigate the risks. The mitigating controls should be tested on a periodic basis to ensure effectiveness.

Risk monitoring

Whenever there is a change in relevant laws or regulations, the GROUP must conduct gap analysis promptly to identify if there is any disparity between the current practice and the new requirements. Action plans need to be formulated accordingly and as appropriate.

Documenting the risk-based strategy

The risk-based approach, including but not limited to the following, must be documented in order to demonstrate to the GROUP or the relevant regulators / authorities:

- Supporting documents on the risk position and assessment including rationale and justification;
- Risk assessment approval note / evidence;
- Application and monitoring; and
- Data, statistic and reporting.

5 RECOGNITION & REPORTING OF SUSPICIOUS CORRUPTION AND UNETHICAL ACTIVITY

Suspicious corruption and unethical activity recognition

All staff is responsible for reporting suspicious activities to the Risk Management Team (“RMT”) of the Group. All internal reported potentially suspicious activities must be reviewed by the RMT of the Group. Staff should be reminded not to tip-off reported individuals (and other non-related parties) and keep the escalated cases confidential.

Suspicious corruption and unethical activity reporting

The Group must observe all legislations and regulations on suspicious corruption and unethical activities reporting and have documented procedures to ensure the reporting procedure and timeline comply with local requirements. Any material cases must be reported to the RMT immediately via e-mail.

Whistleblowing

Employees are encouraged to report or disclose through established whistle blowing channels, concerns about any violations of the Policy, unethical behavior, malpractices, illegal acts or failure to comply with regulatory requirements that is taking place / has taken place / may take place in the future.

The whistleblowing case or concern should be reported via the following channels and person with all the information in details and be as specific as possible which consists of the parties involved, incident date and time, types of concern, evidence substantiating the complaint, where possible, and contact details, in case further information is required:

Chairman of Audit Committee

Independent Non- Executive Director

Email: bs@teoseng.com.my

Mailing address: Lot PTD 25740, Batu 4, Jalan Air Hitam, 83700 Yong Peng, Johor

Employee who makes a report in good faith or assist in an investigation of possible violation will be protected against any form of retaliation. Malicious and false allegations by the whistle blower will be viewed seriously and treated as a gross misconduct and if proven, may lead to dismissal or termination of the whistle blower who abuse this system. The submission and identity of the whistle blower will always be kept in strictest confidentiality.

6 COMMUNICATION, AWARENESS & TRAINING

Induction training on anti-corruption awareness to relevant new staff as well as refresher training to all relevant staff are mandatory. Induction training should be received by all relevant new staff within first four weeks of joining the business and refresher training should be received by all relevant staff at least annually.

All relevant staff should be made aware of and understand:

- The Group's anti-corruption policy;
- The legal obligations and regulatory requirements under which the business operates;
- That they may be held personally liable if they fail to guard against corruption and unethical activity;
- Who serves as RMT, how to contact him/her and the requirement to report any suspicions to him/her;
- The various offences that may constitute corruption and unethical activity;
- Legislations and regulations and other requirements measure and their legal and regulatory obligations and reporting requirements;
- The penalty that may be incurred for failure to comply with relevant requirements.

Employees should receive training appropriate to their roles to enable them to understand the corruption and unethical activity and techniques which are likely to be used in their area of business. In particular, higher risk roles should be determined and additional role's specific training should be designed and rolled out to these higher risk staff. This additional training should be delivered when these staff join the Group and be refreshed annually.

Post-training assessment with a minimum passing score must be implemented in both induction and refresher training to ensure the material is well understood. Case studies using examples from or relevant to the employees' jobs are useful to ensure that the training is appropriate. Training records must be tracked and documented. Completion rate should be monitored to aim for 100% attendance for all relevant staff. Appropriate follow up or disciplinary action should be considered for non-completion of mandatory training unless valid reasons can be obtained.

7 RECORD KEEPING AND INFORMATION SHARING

Records of information including but not limited to the following should be retained to ensure proper audit trail:

- Due Diligence documents including copy of customer identification document, any internal analysis or recommendation, etc;
- Related analysis or recommendation;
- Corruption and unethical activity monitoring and investigation decisions with supporting document
- Risk assessment with supporting documents and approval notes;
- Internal and external anti-corruption reporting documents;
- Anti-corruption training records.

Records of information shall be retained for at least 7 years. The 7 years (or longer) timeframe should be counted from the completion of the event such as suspicious cases reported to authorities.

The Group should establish and maintain procedures for data protection and sharing of information for the purposes of preventing corruption with other members of the Group.