SHCIL SERVICES LIMITED

ANTI-FRAUD POLICY

DOCUMENT CONTROL

Document:	Anti-fraud Policy
For:	SHCIL Services Limited
Classification:	INTERNAL
Version:	Ver 1.**1**
Date:	July, 2018

MESSAGE FROM OUR MANAGING DIRECTOR & CEO

SHCIL Services Limited takes a zero-tolerance approach to fraud, corruption and other malpractices. We are committed to conducting our business with great integrity in a truthful and ethical manner. We wish to promote a culture of honesty, with opposition to frauds in all its forms. We have adopted this policy to communicate this message to all the employees and stakeholders and expect everybody to uphold it.

I encourage you to adhere to these principles in both letter and spirit.

Sanjay Pote
Managing Director & CEO

CONTENTS

1. Background

SHCIL Services Limited (SSL) is committed to protecting the Company's reputation, assets and resources from any attempts of fraud, deceit or any other improper conduct by employees or third parties. The corporate fraud policy is established to facilitate the development of controls that will aid in the detection and prevention of fraud against SSL. It is the intent of our Company to promote consistent organizational behavior by providing guidelines and assigning responsibility for the development of controls and conduct of investigations.

The purpose of this policy is to:

(a) Set out SSL's responsibilities and the responsibilities of those working for SSL or associated with SSL, in observing and upholding our position on fraud & corruption.

(b) Provide information and guidance to those working for SSL on how to recognize and deal with fraud and corruption issues.

(c) Provide guidance, including responsibilities for conducting investigations in fraud-related areas.

(d) Protect employees / entities who may be victimized or harassed as a consequence of reporting or being witness to fraudulent activities.

2. Scope of the policy

The primary objective of this policy is to prevent fraud, enhance the Company's governance and internal controls, standardize business activities, maintain integrity

in the Company's business dealings and establish procedures and guidelines to individuals / entities to detect, act and report fraud / suspicious activities. This policy applies to all individuals working at all levels and grades, including Directors, employees (whether permanent, under contract or temporary), consultants, contractors, casual workers, agency staff, agents, channel partners or any other person associated with SSL, wherever located. Any investigative activity required will be conducted without regard to the suspected wrongdoer's length of service, position/title, or relationship to the Company.

3. Policy

SSL has zero tolerance to fraud and corruption. We strongly discourage all our associated individuals and entities to desist from engaging in any fraud or corrupt practice. All incidents of fraud and corruption are to be reported and investigated. Management is committed to preventing, identifying and addressing all acts of fraud and corruption through raising awareness of fraud risks, implementing controls aimed at preventing and detecting fraud / corruption and enforcing this policy. Fraud is defined as an intentional false representation or concealment of a material fact for the purpose of inducing another to act upon it to his or her detriment. It is also the theft or misuse of Company's funds or other resources by an employee or third party. Actions taken to instigate, aid, abet, attempt, conspire or co-operate in a fraudulent or corrupt act also constitutes a fraud. Each member of the management team will be familiar with the types of improprieties that might occur within his or her area of responsibility, and be alert for any indication of irregularity. Any irregularity that is detected or suspected must be reported immediately to the CFO/Head of Finance of the Company, who coordinates all investigations with the Vigilance Department along with the Legal Department and other involved Departments.

4. Actions constituting fraud

The terms fraud, diversion, falsification, misappropriation, and other fiscal irregularities refer to, but are not limited to:

- Any dishonest or fraudulent act detrimental to the interests of the Company.
- Inappropriate personal use of Company's assets.
- Forging signatures and / or documents, preparing false entries in the system or making false statements to obtain financial or other benefit for oneself or for others.
- Using another person's IT identity or password or creating false identities without consent or authority to manipulate processes.
- Misappropriation of funds, securities, supplies, or other assets.
- Impropriety in the handling or reporting of money or financial transactions.
- Profiteering as a result of insider knowledge of company activities.
- Disclosing confidential and proprietary information to outside parties, other than mandatory disclosures to law enforcement authorities like Police, SEBI, Exchanges, CBI, Courts etc.
- Disclosing to other persons the confidential activities engaged in or contemplated by the company.
- Accepting or seeking anything of material value from contractors, vendors, or persons providing services/materials to the Company in cash or kind.
- Destruction, removal, or inappropriate use of records, furniture, fixtures, equipment, etc.

- Engaging in any activity having similar business objectives amounting to conflict of interest.

Irregularities concerning an employee's moral, ethical, or behavioral conduct should be resolved by departmental management and HWD. If there is any question as to whether an action constitutes fraud, contact the CFO for guidance.

5. Fraud prevention measures

Any form of fraud is costly – both in terms of reputational risk and financial losses, in addition to the time and efforts consumed in identifying and investigating the same. Prevention of fraud therefore, is the key objective of SSL. Appropriate measures and controls are put in place to deny or minimize opportunities for frauds. Some such measures are:

5.1 Awareness sessions

Employees, non-employees, vendors, partners and all related third parties must be aware of their responsibilities to prevent fraud and corruption. Awareness to this can be raised by the Management through circulars, awareness sessions, newsletters, etc. The awareness/ training sessions should cover the modus operandi for frauds that have occurred and the mitigant/ additional controls that would help in preventing their occurrence and limiting their severity if they were to occur.

5.2 Building fraud prevention controls while developing the system

While developing a new program (could be a new Business line or/ and new product/ service offering) or system, it is important to ensure that fraud risks are taken into consideration and appropriate controls are built into it. Program [Business line head or/ and concerned Product/ service head in consultation with the risk management department (RMD)] and project managers (for system implementation after having

received inputs from the business-line head ; i.e. the business line for which the system/ is being implemented and the risk management department and the IT department from IT security and risk management perspective) should be involved since inception and be responsible for ensuring that the risk of fraud and corruption is identified during the design phase. They evaluate the impact and also the effectiveness of the measures taken to mitigate the risks.

5.3 Management of fraud risk

As part of the annual risk and controls self-assessment (RCSA) exercise carried out by the RMD, RMD shall point out fraud risks and recommend mitigant controls in respect of them. The concerned Business-Line heads would be responsible for finalizing these recommended controls or additional ones and provide reasons for not accepting recommended controls. Managers should identify and assess the risk in their respective areas and apply mitigating measures, in consultation with the RMD, based on the level of risk involved. Since it is impossible to mitigate all the risks, a sound risk management strategy involves communication of the residual risks with the relevant stakeholders and accepting such risks. Managers should also be vigilant in monitoring irregularities and the risk of frauds.

For enabling RMD to carry out fraud risk identification/ assessment/ mitigation/ reporting/ management, the concerned business units/ Head-office departments/ (in effect their heads would have this responsibility), shall report fraud occurrences promptly to CFO. Any investigation into fraud event occurrence shall involve the RMD and vigilance department along with any-other unbiased officer/ entity, recommended by senior management.

5.4 Fraud risk assessment

This shall be covered in the annual RCSA exercise conducted by RMD in consultation with business-units. In addition, the business-units/head-office functions (in effect their heads would carry this responsibility) shall carry the onus of reporting fraud event occurrence promptly to RMD, vigilance. Periodic fraud risk assessment should be done to look for new risks that may crop up. All fraud prevention and mitigation measures should be monitored for effectiveness over time, and the fraud risk management process may be repeated periodically utilizing lessons learned, especially in cases where changes have occurred.

5.5 Internal control system

A good internal controls system should be in place where policies and procedures are enforced, and all individuals and responsible parties are made aware about fraud and corruption, besides its consequences. Furthermore, audit programs should include looking for red flags related to fraud and corruption and initiating detailed investigations, wherever warranted. The Internal Audit should also review and monitor the implementation of procedures and controls designed to prevent & detect fraud and issue periodic reports on the effectiveness of the Anti-fraud policy to the Audit Committee of Directors.

5.6 Integrity and industry best practices

Integrity of employees is of paramount importance and should be considered while recruiting employees and while contracting non-staff personnel. Specific interview assessment tools may be used for integrity, academic and professional experience checks.

5.7 Abiding by the Corporate Directives of SSL

Standards / Corporate Directives are established for all staff members. Adherence to the same and strict disciplinary action in the event of non-compliance can deter frauds and encourage higher standards of professional behavior.

5.8 Whistleblower mechanism

Appropriate system should be in place to encourage whistleblowers to share their concerns over unethical activities that they may come across. Issues intimated anonymously will be considered at the discretion of the management depending upon (a) seriousness of the issue (b) credibility of the allegations with supporting facts / evidence (c) the likelihood of confirming and corroborating the allegations through reliable sources.

The identity of the whistleblower will not be disclosed, in case he / she wish to remain anonymous. No retaliatory action would be taken in case the allegations are made in good faith out of genuine concern, even if they turn out to be false. Recognition and awards may also be considered in genuine cases. However, in case individuals make malicious or vexatious allegations, the Company may consider initiating disciplinary action against the individual making the false accusation.

6. Roles and responsibilities

REPORTING OF FRAUD EVENTS

The Departments/ head-office functions (in effect their heads would carry this responsibility) shall carry the onus of reporting fraud event occurrence promptly to RMD, vigilance.

INVESTIGATION OF FRAUD EVENTS

Any investigation into fraud event occurrence shall involve the RMD, vigilance department and along with any-other unbiased officer/ entity, recommended by senior management.

FRAUD RISK MANAGEMENT

RMD shall carry out the annual RCSA exercise, which shall cover fraud risk identification/ assessment/ mitigation as well, in consultation with the business units. In addition, based on fraud event reporting to RMD and others, RMD in consultation with business units, shall convey risk-mitigant/ controls along with timelines within which the control shall get implemented, to prevent occurrence of such risks or/ and reduce their severity if they were to occur.

Concerned Business-unit heads or Head-office department heads, would be responsible for implementing the Controls recommended by RMD within stipulated timelines or provide written reasons for not doing so.

All staff and non-staff personnel have critical roles and responsibilities in ensuring that fraud is prevented, detected and dealt with promptly. They are responsible for safeguarding the resources entrusted to them and for protecting the Company's reputation. They should uphold highest ethical standards and report all acts of fraud and corruption that comes to their notice. They must be aware of the unusual transactions or behaviors that could be indications of fraud. Some of their important roles and responsibilities in this regard are:

- Ensure that the policy is read, understood and complied with at all times.

- Being responsible for the prevention, detection and reporting of frauds and other forms of corruption in their domain and / or under their control. All are required to avoid any activity that might lead to, or suggest, a breach of this policy.
- Notify the Manager or the Compliance Manager as soon as possible, if it is believed or suspected that a conflict with this policy has occurred, or may occur in the future.

Any employee who breaches this policy may face disciplinary action, which could also result in dismissal from service.

7. Investigation Responsibilities

Any investigation into fraud event occurrence shall involve the RMD, vigilance department along with any-other unbiased officer/ entity, recommended by senior management.

SSL Management has the primary responsibility for investigating all suspected fraudulent acts as defined in the policy. The Audit program should include looking for fraud and corruption red flags, besides other risk factors that are consistent with applicable auditing standards. Such cases should be investigated proactively without waiting for receipt of allegations. All allegations of fraud and corruption are to be taken seriously. Upon receipt of an allegation or report, Management will assess the case to ascertain whether there is sufficient ground to warrant an investigation. If the investigation is needed and the same substantiates that fraud has occurred, the Company should issue reports to appropriate designated personnel and, if appropriate, to the Board of Directors through the Audit Committee.

Decisions to prosecute or refer the examination results to the appropriate law enforcement and/or regulatory agencies for independent investigation will be made in conjunction with the legal counsel and senior management.

8. Confidentiality and Non-retaliation

SSL treats all information received as confidential. SSL does not tolerate any form of retaliation against whistleblowers who report in good faith, their concerns relating to known or suspected fraud. SSL will also protect the concerned employee / entity from harassment / victimization. Any employee who suspects dishonest or fraudulent activity will notify the CFO immediately, and should not attempt to personally conduct investigations or interviews / interrogations related to any suspected fraudulent act. Individuals wishing to protect their identity may report fraud anonymously, though this is not strongly encouraged. Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. This is important in order to avoid damaging the reputation of the Company and that of the persons suspected but subsequently found innocent of wrongful conduct, besides protecting the Company from potential civil liability.

9. Authorization for investigating suspected fraud

All investigations conducted by the Investigation Committee authorised by MD & CEO shall be fair and impartial, with due regard to the rights of all the persons or entities involved. All persons or entities shall be deemed innocent unless proven guilty. Members of the Investigation Committee will have:

- Free and unrestricted access to all Company records and premises, whether owned or rented; including CCTV footage, wherever available.

- The authority to examine, copy, and/or remove all or any portion of the contents of files, desks, cabinets, and other storage facilities on the premises without prior knowledge or consent of any individual who might use or have custody of any such items or facilities, if it is within the scope of their investigation. This also includes system-related information stored on PCs, laptops, servers, etc.

All work of the investigating team should be documented, including transcripts of interviews conducted. The conclusion / recommendations of all fraud investigations must be documented.

The person/s who initially reported the suspicious activities may be informed of the outcome of the investigation, but this should be done only after the report and the proposed line of action is finalized.

10. Reporting procedures

REPORTING OF FRAUD EVENTS

The business-units / head-office functions (in effect their heads would carry this responsibility) shall carry the onus of reporting fraud event occurrence promptly to CFO.

All employees should take reasonable steps to prevent the occurrence of fraud and to identify and report instances of known or suspected fraud committed by employees or third parties. All frauds and corrupt practices must be reported. Great care must be taken during the investigation of suspected irregularities so as to avoid mistaken accusations or alerting suspected individuals that an investigation is under way.

Anyone who discovers or suspects fraudulent activity will contact the CFO immediately. The employee or other complainant may remain anonymous. All

inquiries concerning the activity under investigation from the suspected individual, his or her attorney or representative, or any other inquirer should be directed to the CFO or the Vigilance and Legal Department. No information concerning the status of an investigation will be disclosed.

The reporting individual should be advised as under:

- Do not contact the suspected individual in an effort to determine facts or demand restitution.
- Do not discuss the case, facts, suspicions, or allegations with any-one unless specifically asked to do so.

11. Disciplinary action

If an investigation results in a recommendation to initiate disciplinary action against an individual, including termination of service, the recommendation will be reviewed by the designated representatives from Human Resources and the Legal Department and, if necessary, by an outside counsel, before any such action is taken. The final decision w.r.t. disciplinary action including terminate an employee can be made by the Management. In the case of non-staff members who breach this policy, the Company may terminate the contractual relationship with them.

12. Remediation and proactive measures

SSL should use the knowledge gained from audits & investigations of cases involving fraud and corruption to address the potential systemic weaknesses. Reports of risks and vulnerable areas exploited, besides other "lessons learnt" from investigations can be used to improve the system. In such cases, the course of action to be taken to improve the systems should be documented in the investigation report and taken up

for implementation. Appropriate mitigating measures should be taken, including measures to prevent their recurrence.

In cases where the Company has suffered a loss, efforts should be made to recover the same from the individuals / entities who caused the loss, including resorting to legal action, wherever deemed fit.

13. Administration and Review of this policy

This policy may be reviewed periodic basis and approved by the Risk committee of the Board. This Policy is endorsed by the MD & CEO, who is also responsible for the administration, revision, interpretation and application.

****