WHISTLE BLOWER POLICY

1. Introduction

The Board of Directors of SecureKloud Technologies Limited has framed this policy to be known as "Whistle Blower Policy" to promote the highest ethical standards and transparency in the operations of the Company and to facilitate the reporting of potential violations on Company policies and applicable laws. This policy encourages Directors, Employees and Business Associates to raise concerns regarding potential violations including unethical behaviour, actual or suspected fraud or violation of Company's code of conduct without any difficulties and free of any fear of retaliation.

The policy is framed pursuant to Section 177 of the Companies Act, 2013 read with Rule 7 of the Companies (Meetings of Board and its Powers) Rules, 2014 and Regulation 22 of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("LODR Regulations"). SEBI LODR inter-alia, provides, for all listed companies to establish a vigil mechanism / whistle blower policy enabling the Directors, stakeholders, including individual employees, their representative bodies and business associates, to freely communicate their genuine concerns about illegal or unethical practices including instances of leak of Unpublished Price Sensitive Information("UPSI").

2. Objectives

The objective of this Whistle Blower Policy ("Policy") is:

a. to provide employees and business associates a framework and to establish a formal mechanism or process whereby concerns can be raised;
b. to encourage persons to report incidents of unfair and fraudulent practices regarding the Company; and
c. to provide protection to those who report such irregularities or unfair practices including instances of leak of UPSI.

3. Definitions

a. Whistleblower is defined as any Personnel (defined who has or had access to data, events or information about actual, suspected or anticipated Reportable Matter within or by the organization, and, whether anonymously or not), makes or attempts to make a deliberate, voluntary and protected closure or complaint of organizational malpractice.
b. Audit Committee means the Audit Committee constituted by the board of directors of the Company in accordance with Section 177 of the Companies Act, 2013 and Regulation 18 of the Securities and Exchange Board of India (Listing Obligations & and Disclosure Requirements) Regulations 2015, as amended from time to time.
c. Business Associates means vendors associated with the Company and who have dealt with the Company or have been associated with the Company successfully or unsuccessfully in the past.
d. Compliance Officer shall be the Company Secretary of SecureKloud Technologies Limited as appointed under Section 203 of Companies Act, 2013 and Regulation 6 of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations 2015, as amended from time to time.
e. Company shall mean SecureKloud Technologies Limited.

f. Disciplinary Action means any action that can be taken on the completion of / during the investigation proceedings including but not limiting to a warning, imposition of fine, suspension from official duties or any such action as is deemed to be fit considering the gravity of the matter.

g. Employee means every employee of the Company and includes ~~working in India or abroad and includes employees of the Companies' Subsidiaries,~~ contract employees, consultant, fixed term employment.

h. Personnel means any employee, director, officer, customer, contractor and/or third-party intermediary engaged to conduct business on behalf of the Company, such as agents and consultants.

i. Reportable Matters means any Company matters involving abuse of authority, breach of the Company Code of Conduct, fraud, bribery, corruption, employee misconduct, illegality, accounting, financial or auditing issues, health & safety, environmental issues, wastage / misappropriation of company funds/assets, leakage of UPSI and any other unethical conduct.

j. Unpublished Price Sensitive Information or "UPSI" means any information as defined in the Securities and Exchange Board of India (Prohibition of Insider Trading) Regulations, 2015, relating to the Company's securities, directly or indirectly, that is not generally available which upon becoming generally available, is likely to materially affect the price of the securities and shall, ordinarily including but not restricted to, information relating to the following: -

   i. financial results;
   ii. dividends;
   iii. change in capital structure;
   iv. mergers, de-mergers, acquisitions, delisting, disposals and expansion of business and such other transactions;
   v. changes in key managerial personnel;
   vi. issue of shares (preferential or bonus or otherwise)

k. Vigil Mechanism Officer means an officer who is/are nominated/ appointed to conduct detailed investigation of the disclosure received from the whistleblower and recommend disciplinary action. Currently, Mr. Thyagarajan R, Whole-time Director and Chief Financial Officer is nominated as Vigil Mechanism Officer.

4. Scope of Policy

The Policy covers any concern with respect to unlawful or unethical or improper practice or act or activity that could have grave impact on the operations, performance of the business or reputation of the Company and may include, but is not limited to, any of the following:

i. Fraud (an act of willful misrepresentation which would affect the interests of the concerned) against investors, securities fraud, mail or wire fraud, bank fraud or fraudulent statements to the Securities and Exchange Board of India (the 'SEBI'), the relevant stock exchange and any other relevant authority.

ii. Violations of any rules and regulations applicable to the Company and related to accounting, internal accounting controls and auditing matters

iii. Intentional error or fraud in the preparation, review or audit of any financial statement of the Company.
iv. Abuse of authority by an employee or biased or favoured approach or behaviour
v. Breach of contract with the company
vi. Negligence causing substantial and specific danger to public health and safety and the environment;
vii. Manipulation of company data /records;
viii. Disclosure of confidential / proprietary information to unauthorized personnel;
ix. Criminal activity or offence affecting operations or functioning of the Company;
x. Wastage/misappropriation of company funds/assets;
xi. Breach of Code of Conduct of the Company or the Policy for Prevention of Sexual Harassment or any other rule or Policy as may be formulated by the Company from time to time;
xii. Leak of UPSI;
xiii. Any other event which would affect the interests of the business; and
xiv. Any other unethical, biased, favoured or fraudulent activity.

5. Committee

The Vigil Mechanism Committee of the Company shall comprise of:

i. Thyagarajan R, Whole-time Director and CFO – Vigil Mechanism Officer
ii. Siva Kumar, Chief Delivery Officer and HR
iii. Vignesh Lingappan, Manager-Finance
iv. Roshini Selvakumar, Company Secretary

6. Disqualification

This Policy should not be misused by any person to make frivolous or malicious or bogus disclosures to the Vigil Mechanism Committee. Whistle Blowers, who make a minimum of two (2) Protected Disclosures, which have been subsequently found to be frivolous or bogus with malafide intent, will be disqualified from reporting under this Policy for such period as Vigil Mechanism Officer may decide. The Vigil Mechanism Committee may impose a penalty or decide such Disciplinary Action, as it deems fit, may be taken against such Whistle Blowers.

7. Reporting

Reporting is the first crucial step to initiate action for early detection, proper investigation and remediation, and deterrence of violations of Company policies or applicable laws. Every Director, Employee and Personnel are empowered under this Policy to report to the Vigil Mechanism Committee any of the Reportable Matters of which they are or become aware of, to the Company. This Policy is intended to encourage and enable personnel to raise serious concerns within the Company prior to seeking resolution outside the Company. The Company does not tolerate any statutory non-compliance or wrongdoing, malpractice and impropriety. This Policy ensures that Personnel are empowered to pro-actively bring to light such instances without fear of reprisal, discrimination or adverse employment consequences.

8. Process of Reporting

A Whistle Blower should raise Reportable Matters at the right moment to address them appropriately. A Whistle Blower must report all suspected Reportable Matters other than matters pertaining to accounting or financial reporting, insider trading in the order of:

i. Vigil Mechanism Officer
ii. Audit Committee

A Whistle blower must report all suspected Reportable Matters pertaining to accounting or financial reporting, insider trading directly to the Company Secretary who shall forward the report to the chairman of the Audit Committee within 24 hours of receipt of the report.
A complaint may be made anonymously. However, the complainant must be detailed in their description of the complaint and must provide the basis of making the assertion therein. It is essential for the Company to have all critical information in order to enable the Company to effectively evaluate and investigate the complaint.
All reporting under this policy should include as much information about the suspected violation. Where possible, it should describe the nature of the suspected violation; the identities of persons involved in the suspected violation; a description of documents that relate to the suspected violation; and the time frame during which the suspected violation occurred.

9. Disclosures

A disclosure should be made in writing. Letters can be submitted by hand-delivery, courier or by post addressed to the Vigil Mechanism Officer. Emails can be sent to the email ID: rt@securekloud.com, a disclosure should normally be submitted to the Vigil Mechanism Officer. It may also be submitted directly to the Chairman of the Audit Committee when the Whistleblower feels it necessary under the circumstances. In such a case, it could be mailed to biju.chandran@securekloud.com
The following details MUST be mentioned:

a. Name, address and contact details of the Whistleblower (including employee code, if the Whistleblower is an employee).
b. Brief description of the Malpractice, giving the names of those alleged to have committed or about to commit a Malpractice. Specific details such as time and place of occurrence are also important.
c. In case of letters, the disclosure should be sealed in an envelope marked "Whistle Blower" and addressed to the Vigil Mechanism Officer OR Audit Committee depending on position of the person against whom disclosure is made.

10. Process after disclosure and Investigation

(a) The Vigil Mechanism Officer/Company Secretary shall acknowledge receipt of the Disclosure as soon as practical (preferably within 07 days of receipt of a Disclosure), where the Whistleblower has provided his/her contact details.
(b) The Vigil Mechanism Officer along with the Vigil Mechanism Committee will proceed to determine whether the allegations (assuming them to be true only for the purpose of this determination) made in the Disclosure constitute as a Malpractice by discussing with the Committee (if required). If the Committee determines that the allegations do not constitute a Malpractice, he/she will record this finding with reasons and communicate the same to the Whistleblower.
(c) If the Vigil Mechanism Officer along with the Vigil Mechanism Committee determines that the allegations constitute a Malpractice, he/she will proceed to investigate the Disclosure with the

assistance of the representative of the Division/ Department where the breach has occurred, as he/she deems necessary. If the alleged Malpractice is required by law to be dealt with under any other mechanism, the Vigil Mechanism Officer shall refer the Disclosure to the appropriate authority under such mandated mechanism and seek a report on the findings from such authority.

(d) Subjects will normally be informed of the allegations at the outset of a formal investigation and have opportunities for providing their inputs during the investigation.

(e) The investigation may involve study of documents and interviews with various individuals. Any person required to provide documents, access to systems and other information by the Vigil Mechanism Officer for the purpose of such investigation shall do so. Individuals with whom the Vigil Mechanism Officer requests an interview for the purposes of such investigation shall make themselves available for such interview at reasonable times and shall provide the necessary cooperation for such purpose.

(f) If the Malpractice constitutes a criminal offence, the Vigil Mechanism Officer will bring it to the notice of the Audit Committee and take appropriate action including reporting the matter to the police.

(h) The Vigil Mechanism Committee shall conduct such investigations in a timely manner and shall submit a written report containing the findings and recommendations to the Audit Committee as soon as practically possible and in any case, not later than 90 days from the date of receipt of the Disclosure.

(i) Whilst it may be difficult for the Vigil Mechanism Officer to keep the Whistleblower regularly updated on the progress of the investigations, he/she will keep the Whistleblower informed of the result of the investigations and its recommendations subject to any obligations of confidentiality.

11. Confidentiality

All reports under this Policy will be promptly and appropriately investigated, and all information disclosed during the investigation will remain confidential, except as necessary to conduct the investigation and take any remedial action, in accordance with applicable law. Everyone working for or with the Company has a duty to cooperate in the investigation of reports of violations. Failure to cooperate in an investigation, or deliberately providing false information during an Investigation, can be the basis for disciplinary action, including termination of employment. If, at the conclusion of its investigation, the Committee determines that a violation has occurred, it may take effective remedial action commensurate with the nature of the offense. This action may include disciplinary action against the party, up to and including termination. Reasonable and necessary steps will also be taken to prevent any further violations of Company policy.

12. Zero Tolerance to Retaliation

No Personnel shall suffer reprisal, discrimination or adverse employment consequences who in good faith, makes a disclosure or lodges a complaint in accordance with this Policy, or participating or assisting in the investigation of, a reasonably suspected violation of any law, this Policy, or the Company's Code of Conduct and Ethics. The Company takes reports of such retaliation seriously. Incidents of retaliation against any Personnel reporting a violation or participating in the investigation of a reasonably suspected violation will result in appropriate disciplinary action against anyone responsible, including possible termination of employment or civil, criminal and administrative penalties.

13. Communication on leak Of Unpublished Price Sensitive Information

Employees are advised to report instances of any leakage of any Unpublished Price Sensitive information (UPSI) to the Compliance Officer of the Company either orally or through written communication or through e-mail to cs@securekloud.com

14. Document Retention

All documents related to reporting, investigation and enforcement pursuant to this Policy shall be kept in accordance with the Company's record retention policy and applicable law.

15. Modification

The Audit Committee or the Board of Directors of SecureKloud can modify this Policy unilaterally at any time without notice. Modification may be necessary, among other reasons, to maintain compliance with the regulations and / or accommodate organizational changes within the Company.

16. Conclusion

The severity of violations may not be assessed unless the issues get escalated that could subject the Company and any individual employee to face penal consequences both within the organization and society as a whole. Before the issues are escalated to that level, Personnel are encouraged to report any violations covered hereinabove at appropriate time under this Policy without any fear of reprisal or discrimination or adverse employment consequences.