Whistle blowing policy

1. PURPOSE

1.1. This Whistleblowing Policy (the "Policy") aims to:-

1.1.1 provide a reliable avenue for persons to report any wrongdoings including suspected violation of Sembcorp Energy India Ltd ("Company" or "SEIL")'s Code of Business Conduct or any applicable law or policy without fear of reprisals when whistleblowing in good faith; and,

1.1.2 ensure that arrangements are in place to facilitate independent investigation of the reported concern and for appropriate follow up actions to be taken.

1.2 The Policy is formulated pursuant to Section 177 of the Companies Act, 2013 and Regulation 22 of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015.

1.3 The effective implementation of this Whistleblowing Policy will be overseen by the SEIL Audit Committee. This SEIL Audit Committee will be assisted by the Investigation Owner(s) (see Appendix 1), the Whistleblowing Committee and Internal Audit when investigating a reported issue and taking follow up action.

2 SCOPE

2.1 This Policy applies to all persons, including employees (i.e. the Board of Directors, officers, full-time/ part-time/ permanent/ contract employees) working for SEIL.

3 POLICY REFERENCE

3.1 Employees should note that this Policy covers all reportable concerns, including violation of all policies issued by SEIL and respective business units.

4 DEFINITIONS

4.1 Compliance with this policy is monitored by Internal Audit which in turn reports to the SEIL Audit Committee. The following SEIL personnel involved in the whistleblowing process are:

4.1.1. Whistleblower – The Whistleblower is central to the Whistleblowing Policy. The Whistleblower is any person who reports any kind of information or activity that is deemed illegal, unethical or not correct within the Company through SEIL's whistleblowing channels. This information of alleged wrongdoing can be classified as violation of company policy/rules, laws, regulations, as well as fraud and corruption. Any adverse action taken against a person for filing a complaint under this whistleblowing policy or supporting another person's complaint is also addressed in Appendix 1.

4.1.2. SEIL Whistleblowing Committee comprises of key representatives from SEIL Governance and SEIL Human Resources, with Head of Internal Audit as the chairperson on this SEIL Whistleblowing Committee. Unless otherwise stated in this Policy, the SEIL Whistleblowing Committee has a high level supervision of all investigations and the Head of Internal Audit is the chairperson of the SEIL Whistleblowing Committee.

4.1.3. Investigation Owner is the department who has main responsibility in ensuring that a reported concern is dealt with appropriately and following up on the status of any recovery, remediation and/ or disciplinary action. The Investigation Owner shall provide the status and investigation report relating to any reported concern to the Internal Audit for quarterly reporting to the SEIL Audit Committee. In cases where Internal Audit receives a reported concern, it shall be redirected to the respective Investigation Owner.

4.1.4. Investigation Team – When dealing with a reported concern, the Investigation Owner may appoint an Investigation Team to conduct investigation into suspected violation of Code of Business Conduct or any applicable law or policy. Depending on the nature of the reported concern and subject matter expertise required, the Investigation Owner may staff the Investigation Team with individuals from different functions or external consultants to assist with either certain elements of the investigation or the whole investigation process.

5 REPORTABLE CONCERN

5.1 Employees are encouraged to come forward to report any situation that involves a violation of the Code of Business Conduct or any applicable law or policy (known as "reportable concern"). Appendix 1 sets out a list of what constitutes reportable concerns, and their respective Investigation Owners.

6 COMMUNICATION AND CLARIFICATION OF THIS POLICY

6.1 This Policy shall be communicated to Employees of SEIL as follows:

6.1.1 To all new Employees during onboarding;

6.1.2 To all Employees as part of compulsory refresher trainings; and

6.1.3 As and when requested by SEIL Audit Committee or SEIL Board of Directors.

6.2 At any time, if an Employee is unclear about whether an action is lawful or complies with Company policies, laws or regulations, such Employee is invited to seek clarifications or advice.

6.3 Depending on the circumstances, Employees may seek clarifications or advice from the respective Policy Owner, Division Heads, Department Heads, Supervisors, Human Resources, or Internal Audit.

7 WHEN TO REPORT

7.1 All Employees have a duty to report a concern as soon as he/she become aware of a situation that may involve a violation of the Code of Business Conduct or any applicable law or policy. Doing so may help the Company prevent illegal or unethical misconduct, or may prevent a situation from escalating. Failure to report a violation may subject the Employee to a disciplinary action up to and including termination of employment.

7.2 Although the whistle-blower is not expected to prove the truth of an allegation, he/ she needs to demonstrate that there are sufficient grounds for concern.

8 WHISTLEBLOWING CHANNELS

8.1 All persons can report their concerns to the Internal Audit via giaindia.cases@sembcorp.com or telephone at +91-9845702875.

8.2 In the event that an Employee receive a reportable concern in the course of his/her work, either via post, email, phone call or in-person, he is required to re-direct the reportable concern to the Head of Internal Audit immediately for appropriate action to be taken.

8.3 Whistle-blowers who report their concerns should provide the following details to assist the Internal Audit in assessing the credibility of the allegations:

8.3.1 Your name and contact details

8.3.2 Your relationship with SEIL

8.3.3 Names of the people and/or organizations involved

8.3.4 The details of the incident (what happened, where and when did it occur)

8.3.5 Whether management has been notified (if so, whom)

8.3.6 How you got to know of the incident

8.3.7 Provide supporting evidence

9 CONFIDENTIALITY AND NON-RETALIATION

9.1 Whistle-blowers are encouraged to provide their names and contact details in confidence, rather than anonymously.

9.2 While SEIL recognizes that information from anonymous source is just as important to act upon, an anonymous Whistle-blower should be aware that the ability of the Internal Audit to ask follow-up questions and address his/ her concerns will be limited if he/she cannot be contacted.

9.3 The identity of the Whistleblower will be kept confidential, with disclosure on a need-to-know basis.

9.4 The Investigation Owner will seek the whistleblower's consent prior to disclosing his/ her identity to anyone other than the aforementioned parties.

9.5 SEIL does not tolerate the harassment or victimization of anyone who reports a concern in good faith. Such conduct is itself a breach of the Code of Business Conduct and anyone who engaged in retaliation against someone who reports a concern will face disciplinary action, up to and including termination, regardless of that person's position or stature within the Company.

9.6 In the event where it is determined that a whistleblower was subject to retaliatory actions, SEIL Whistleblowing Committee will undertake appropriate remedial actions under SEIL Audit Committee's directives.

10 FRIVOLOUS AND MALICIOUS WHISTLEBLOWING

10.1 SEIL treats all reported concerns seriously and will direct resources towards investigation and monitoring of these cases. The Company does not wish for any employee to misuse the whistleblowing channels and does not condone frivolous and/ or malicious whistleblowing.

10.2 If the results of the investigation show that the Employee has acted maliciously in reporting his/ her concern, he/ she will be subject to disciplinary action up to and including termination of employment.

10.3 Examples of frivolous and malicious whistleblowing includes, but is not limited to:

10.3.1 having no reasonable grounds to believe that the information he/ she provided was true and accurate; or

10.3.2 knowingly spreading false information with the intent to damage another party's reputation or cause distress to that party.

11 HANDLING A REPORTABLE CONCERN

11.1 SEIL treats all reports of suspected violation of the Code of Business Conduct or any applicable law and policy seriously. Each report will be reviewed by the Internal Audit based on established procedures. The Company strives to conduct each case with impartiality, fairness and confidentiality.

11.2 SEIL respects the rights of all parties involved in potential fraud and misconduct and will handle all reports with discreteness during the course of investigation.

11.3 SEIL will take reasonable steps to ensure that that the identity of the alleged violator(s) is kept confidential, with disclosure on a need-to-know basis and/or as required under any applicable law.

12 COOPERATION

12.1 Employees who are interviewed or asked to provide information have a duty to fully cooperate with the Investigation Team. All persons should refrain from making speculations, discussing or disclosing matters concerning the investigations.

12.2 At the recommendation of the Investigation Team, the Company may undertake any disciplinary action up to and including termination of employment against any Employee who fails to cooperate with an investigation.

13 SUSPENSION OF EMPLOYMENT, BONUS AND INCREMENT

13.1 During an investigation, the Company may suspend an alleged Employee from work during the investigation period where permissible under local employment agreement and laws. If the investigation does not disclose any misconduct on the part of the Employee, the Company shall restore to the Employee the full amount of salary withheld.

13.2 Employees who are under investigation will have their variable bonus and salary increment withheld for the period of the investigation. The variable bonus and/or salary increment shall be reinstated to the Employee only if the Employee is cleared of any misconduct.

14 PRESERVATION OF EVIDENCE

14.1 The Investigation Team may issue a preservation notice and appoint a Custodian to take-over and preserve evidence for the purposes of the investigation including, but not limited to electronic data and physical documents.

14.2 All Employees, regardless of position or stature, are expected to comply with the preservation notice and handover the required evidence to the designated Custodian. Employees shall not alter, destruct or delete the evidence covered under this preservation notice without written approval from the Head of Internal Audit.

14.3 Any Employee who is found to be in violation of the preservation notice will be subject to disciplinary actions up to and including termination of employment.

15 ACCESS TO INVESTIGATION DETAILS AND REPORTS

15.1 Any investigation details, reports and resulting actions are considered privileged and confidential information. Distribution and access to such information are restricted to the SEIL Audit Committee, SEIL Whistleblowing Committee and the Internal Audit. The SEIL Audit Committee may grant access of such confidential information at its discretion, on a need to know basis.

15.2 Persons who have access to the investigation details and reports shall not disseminate such information without written consent from the SEIL Audit Committee and/or Head of Internal Audit. Examples of such investigation details include, but is not limited to:

15.2.1 Names of the whistleblower and alleged person/company against whom the report is made;

15.2.2 Nature of the allegations;

15.2.3 Investigation approaches;

15.2.4 Investigation Team's travel schedule and physical location;

15.2.5 Information requests and details of discussions conducted with the Investigation Team.

15.3 Any person found to be in breach of 15.2, is deemed to have jeopardized the investigation or put the safety of the Investigation Team at risk. Employees shall be subject to disciplinary actions, up to and including termination of employment.

16 FUNDING APPROVAL FOR EXTERNAL RESOURCES

16.1 From time-to-time, the Internal Audit will engage external resource(s), including but not limited to legal counsel, forensic professionals and expert witnesses to conduct investigations. Justifications and details of engagement of such external resources are considered highly sensitive and confidential information, with access restricted to the SEIL Audit Committee and Internal Audit.

16.2 The purchase requisitions, contracts and invoices with respect to an investigation shall be subject to the sole review and approval of the SEIL Audit Committee and relevant documents will be released to the respective departments as supporting documentation after conclusion of the investigation. Upon approval by the SEIL Audit Committee, the relevant departments and business units should ensure that funding and payments are provided to the Investigation Team on a

timely basis to facilitate the engagement of such external resource(s).

17 REPORTING TO REGULATORS AND LAW ENFORCEMENT AUTHORITIES

17.1 SEIL adopts a zero tolerance approach towards non-compliance with its Code of Business Conduct, as well as the applicable laws and policy. Where there are reasonable grounds to suspect any criminal conduct or regulatory violation that attracts civil or criminal sanctions, the Company will make the relevant disclosures and/or file a case with the relevant regulators and/or law enforcement authorities upon consultation with the SEIL Board of Directors and SEIL Audit Committee.

18 RECOVERY, REMEDIATION AND DISCIPLINARY ACTIONS

18.1 The respective business units are expected to undertake any recovery and remediation actions identified by the Investigation Team subsequent to an investigation.

18.2 Any disciplinary actions arising from an investigation will be determined by the Whistleblower Committee, of which SEIL Human Resources is a member, and be communicated to the respective business units.

The Internal Audit will escalate any delays or inaction towards recovery, remediation and disciplinary actions to the SEIL Audit Committee and SEIL Board of Directors.

APPENDIX 1 – LIST OF REPORTABLE CONCERNS

Type	Description	Investigation Owner
Category A: Bribery & corruption, fraudulent accounting, embezzlement and anti-trust/ competition		
1. Bribery and corruption	❖ Offering or providing items of value to anyone, including a government official in order to influence them into granting deals/ contracts or other favours in furtherance of the Company's business. ❖ Soliciting for items of value from any outside parties who have or would like to establish a relationship with the Company, other than potential/ existing suppliers or service providers (which fall under the procurement fraud category). ❖ Items of value includes money, gifts, gratuities, loans, fees, rewards, employments, contracts, discounts, services, entertainment, accommodation, favours, or services.	Internal Audit
2. Fraudulent Accounting	❖ Financial transactions that are not in compliance with local GAAP, or containing false, misleading or incomplete entries or records.	Internal Audit
3. Embezzlement	❖ Taking property entrusted in one's care for personal benefit, or making unauthorised/improper payments to third parties.	Internal Audit
4. Travel and expense	❖ Includes, but it not limited to, submitting false receipts, submitting receipts for personal expenses as business expenses, and submitting expenses for reimbursement that are not permitted under Corporate policy.	Internal Audit
5. Procurement fraud	❖ Includes, but not limited to: receiving any direct/ indirect payment, gifts from any potential/ existing suppliers or service providers of the Company in exchange for business or to influence any action/ decision; • having an undisclosed relationship with, or a personal, or financial interest in potential/ existing suppliers or service providers, or any situation that could cause real or perceived divided loyalty; • tender irregularities;	Internal Audit

	• manipulation of purchase quotations; • unfair advantage to potential/ existing suppliers or service providers; • non-compliance with procurement policy and procedures; • product substitution; • cost/labour mischarging services,	
6. Anti-trust/ competition law	❖ A practice or arrangement that either prevents or restricts fair competition that is in contrary to local anti-trust law. ❖ Examples include: Oral/written agreements, arrangements or understandings with other business parties to fix prices, boycott specific suppliers or customers, allocate territories/ market, exchange competitively sensitive information, discuss on price/ rebates/costs/marketing plans and other confidential information.	Internal Audit
Category B: Theft and misuse of company assets		
7. Asset theft	❖ Stealing or unauthorised taking/ removing of company's property with the intent to deprive the rightful owner of it.	Internal Audit
8. Misuse of company assets	❖ Using the company's assets for personal or improper use. This includes, but is not limited to, company computers, phones, printers, office supplies, and other company property.	Internal Audit
9. IT security	❖ Misuse of company's computer systems, or unauthorized access of data, applications, networks and/or devices. ❖ Examples include, but not limited to failure to protect and maintain the integrity of data stored on the Company's information technology assets or networks, accessing data using another Employee's password.	Internal Audit
10. Confidentiality and intellectual property	❖ Unauthorised use or unauthorised disclosure of confidential information. Examples of confidential information includes but not limited to: company's business and marketing plans, contracts and details of its computer systems. ❖ Unauthorised or improper use a third party's	Internal Audit

	intellectual property rights, including patents, trademarks, copyrights and trade secrets.	
Category C: Conflict of interest, personal data privacy, employment relations and other inappropriate behaviours		
11. Conflict of interest	❖ A situation in which an Employee, has a private or personal interest sufficient to appear to influence the objective exercise of his or her official duties. ❖ Examples include: undeclared financial interest in a supplier or party that does business with the Company, engaging covertly in the production of services or goods in competition with the Company, favourable treatment of a particular job applicant or customer or subordinate for personal reasons.	Internal Audit/ Human Resources.
12.Personal data privacy	❖ Violation of Employee data privacy law in the collection, maintenance, access, transfer, disclosure and/or destruction of Employee sensitive data.	Data Protection Officer
13.Employment relations	❖ Issues involving violation of local labour laws or employment eligibility requirements. ❖ This includes but not limited to: • use of child labour;	Human Resources
	• falsification of employment application; • hiring bias; • issues concerning quantity of hours worked, overtime pay, rest periods; • inaccurate, late or non-payment of wages; and • wrongful termination.	

14. Misconduct or inappropriate behaviour, discrimination/ harassment	❖ Such behaviours include, but not limited to: • insubordination; • violence; • offensive language/actions; • threats/intimidation; • time and attendance fraud; • possession or use of alcohol and drugs within company premises; • damage to company's property/equipment; • hindering of company operations; • posting of malicious or sensitive comments on suppliers/ customers/employees in the social networking sites; • misrepresenting company's position in social networking sites; • uninvited and unwelcome verbal or physical conduct directed at an Employee because of his or her sex, religion, disabilities, family status, ethnicity, or beliefs; • sexually offensive gestures; and • pressurising a fellow Employee for sexual favours.	Human Resources
Category D: Retaliatory actions, HSE, securities violation and others		
15. Retaliatory actions	❖ Engaging in retaliatory conduct against a whistle-blower who has reported through the whistleblowing channels in good faith.	Respective investigation owner or an independent party
	❖ Examples include: • actions causing injury, loss or damage; • intimidation or harassment; • Disciplinary actions, discrimination, disadvantage or adverse treatment in relation to the whistle-	

	blower's employment and/or career.	
16. Environmental protection, health and safety	❖ Failure to meet environmental regulations, corporate policy or procedure that have adverse impact on the health and general well-being of Employees/overall community ❖ Examples include: environmental damage, poor housekeeping, fire or explosion hazards, improper use of equipment, inappropriate protective clothing.	HSE Compliance Audit Team[1]
17. Securities violation	❖ An infringement of the Singapore Exchange (SGX)/Securities Exchange Board of India (SEBI) listing rules. ❖ Example include: insider trading.	Internal Audit
18. Others	❖ All other forms of misconduct or fraud, or violation of corporate policies, laws and regulations that does not fit into the aforementioned allegation categories.	Internal Audit