

VIGIL MECHANISM / WHISTLE BLOWER POLICY

I. Introduction

Cybertech Systems and Software Limited (“Company”) believes in conduct of the affairs of its constituents in a fair and transparent manner by adopting highest standards of professionalism, honesty, integrity and ethical behavior. The Company is committed to develop a culture where it is safe for all employees to raise concerns about any fraudulent or unacceptable practice and any event of misconduct. **Vigil Mechanism / Whistle Blowing Policy (The Policy)** is a devise to help alert and responsible individuals to bring to the attention of the Management, promptly and directly, any unethical behavior, suspected fraud or abrasion or irregularity in the Company practices which is not in line with Code of Business Principles or the law of the land, without any fear or threat of being victimised.

This Policy is issued 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 clause 49 of the Listing Agreement.

Mechanism shall provide for adequate safeguards against victimisation of employees and directors who avail of such mechanism and also provide for direct access to the Chairperson of the Audit Committee or the Director nominated by the Audit Committee, as the case may be, in exceptional cases.

II. Address for Communication:

The Whistle Blower shall send his/her Grievance/concern/Complaint/irregularities (“Concern”) by sending a mail to E-mail to the Compliance Officer at sarita.leelaramani@cybertech.com

Alternatively he/she may write a letter addressed to the following address.

Sarita Leelaramani
Company Secretary
CyberTech Systems and Software Limited,
CyberTech, Plot No. BV-63/64,65
Road No. 21/34, J.B. Sawant Marg,
MIDC, Wagle Estate,
Thane (West)-400 604

The Concern raised will be placed by the Executive Director before an Internal Committee for investigation. The Committee will investigate the Concern and if it finds

no merit or materiality in the Concern, the said Concern will be closed and intimation will be sent to Whistle Blower within reasonable period of 30 days from the receipt of Concern. The Committee may give an opportunity of being heard to the Whistle Blower on the principles of natural justice.

However if the Committee finds merit in the concerns raised may call for an independent inquiry which will be referred to the External Auditor or Audit Committee or any external agency.

On receipt of the outcome of the external investigation, a further decision will be taken by the Audit Committee. However for any further criminal action, Chairman of the Company will take a final decision whether to refer the matter to Police or not.

III. Protection

- A) No unfair treatment will be given to a Whistle Blower by virtue of his/her having reported a Protected Disclosure under this Policy. The Company, as a policy, condemns any kind of discrimination, harassment, victimization of Whistle Blower. Complete protection will, be given to Whistle Blower against any unfair practice like threat or termination / suspension of service, disciplinary action, or the like including any direct or indirect use of authority to obstruct the Whistle Blower's right to continue to perform his duties/functions including making further Protected Disclosure.
- B) The Company will do its best to protect an individual's identity when s/he raises a concern and does not want their name to be disclosed.
- C) If the Whistle Blower makes an allegation in good faith, which is not confirmed by the investigation, no action will be taken against the Whistle Blower. If a complaint is malicious or vexatious, disciplinary action will be taken.
- D) This Policy encourages individuals to put their names to allegations. However, individuals may raise concerns anonymously. Concerns expressed anonymously will be evaluated by the Company for investigation. In exercising this discretion, the factors to be taken into account would include:
 - The seriousness of the issue raised;
 - The credibility of the concern; and
 - The likelihood of confirming the allegation from attributable sources

IV. Reporting:

- A quarterly report with number of complaints received under the Policy and their outcome shall be placed before the Audit Committee and the Board periodically.

- Details of establishment of such mechanism shall be disclosed by the Company on its website, if any, and in the Board's report.

V. Coverage of Policy:

The Policy covers malpractices and events which have taken place/ suspected to take place involving:

1. Abuse of authority
2. Breach of contract
3. Negligence causing substantial and specific danger to public health and safety
4. Manipulation of company data/records
5. Financial irregularities, including fraud, or suspected fraud
6. Criminal offense
7. Pilferation of confidential/propriety information
8. Deliberate violation of law/regulation
9. Wastage/misappropriation of company funds/assets
10. Breach of employee Code of Conduct or Rules
11. Any other unethical, biased, favoured, imprudent event

Notes:

- i. Policy should not be used in place of the „Company grievance procedures“ or be a route for raising malicious or unfounded allegations against colleagues.
- ii. Protection under this Policy would not mean protection from disciplinary action arising out of false or bogus allegations made by a Whistle Blower knowing it to be false or bogus or with a *mala-fide* intention.
- iii. Whistle Blowers, who make any Protected Disclosures, which have been subsequently found to be *mala-fide*, frivolous or malicious shall be liable to be prosecuted under Company's Code of Conduct.