VIGIL MECHANISM (WHISTLEBLOWER) POLICY

Mungi Engineers Pvt. Ltd. | Mungi MetalCraft LLP

Policy Code: POL/HR/MEPL-MMC/01
Edition: 1.0 | **Revision:** 0
Approved by: Board of Directors
Effective Date: 13/11/2025
Next Review: Annually (or earlier as required)
Owned by: Whistleblower Officer (GM–HR) & Audit Committee

Table of Contents

---

1. Preamble / Legal Basis

Mungi Engineers Pvt. Ltd. and Mungi MetalCraft LLP (together, the "Company") are committed to the highest standards of ethical, legal and regulatory conduct. This Vigil Mechanism (Whistleblower) Policy is established in accordance with Section 177 of the Companies Act, 2013 and Rule 7 of the Companies (Meetings of Board and its Powers) Rules, 2014, and is drafted to reflect current national and international best practice (including guidance from ISO 37002). Where applicable, this Policy is designed to meet additional statutory or regulatory requirements (for example, listing rules) and to operate consistently with the Company's other governance policies.

Note: The public/website version of this Policy will exclude personal home addresses and personal contact details. Corporate contact information and hotline details (or the process to obtain them) will be published instead.

2. Purpose

To provide an accessible, safe and confidential mechanism for directors, employees and other stakeholders to report concerns about wrongdoing (including but not limited to fraud, corruption, financial irregularities, serious legal or policy breaches, threats to health and safety, environmental harm, quality or product safety issues), and to ensure that such reports are assessed and investigated impartially, fairly, and in a timely manner with appropriate remediation and protections for good-faith reporters.

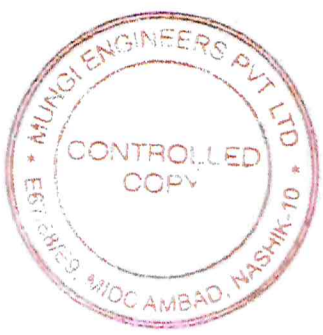
3. Scope

This Policy applies to: - All employees (full-time, part-time, temporary, contract, outsourced) of the Company and its subsidiaries;
- Directors (executive and non-executive);
- Contractors, vendors, suppliers, consultants and other third-party associates;
- Customers, shareholders and other external stakeholders where relevant.

Reports relating to subsidiaries or other third parties providing services to the Company are covered where the reported conduct affects the Company's operations, reputation or regulatory compliance.

3A. Relationship with Other Company Policies

This Policy complements and does not replace other procedures such as the HR Grievance Policy (routine employment issues), POSH policy (complaints of sexual harassment handled per the POSH Act 2013), quality management processes (IATF/ISO where applicable) and other compliance policies. Where a disclosure concerns matters covered primarily by another policy, the Whistleblower Officer will coordinate appropriate referral while ensuring protection and confidentiality for the reporter.



4. Definitions

- **Whistleblower / Complainant:** Person making a Protected Disclosure under this Policy.
- **Protected Disclosure:** A report made in good faith that discloses or demonstrates information that may indicate unethical, illegal or improper activity.
- **Subject:** Person(s) against whom the Protected Disclosure is made.
- **Whistleblower Officer (WBO):** Nodal officer responsible for intake and coordination of the process (see Section 9).
- **Whistleblower Committee / Investigation Team:** Team (internal and/or external) designated to investigate a disclosure.
- **Good Faith:** A reasonable belief, based on objective grounds, that the information disclosed is true. Malicious or knowingly false allegations are not made in good faith.

5. Principles & Standards

This Policy is guided by the following principles: - **Confidentiality & Privacy:** The identity of the reporter, subjects and witnesses will be protected to the maximum extent possible, consistent with proper investigation and applicable law.
- **Protection from Retaliation:** No retaliation will be tolerated against any person reporting concerns in good faith.
- **Impartiality & Fairness:** Investigations will be objective, documented and proportionate.
- **Accessibility:** Multiple channels will be available for reporting, including the option to report anonymously.
- **Proportionality & Due Process:** Any action taken against a Subject will be based on evidence, follow natural justice, and allow an opportunity to respond.

6. Reporting Channels

The Company provides multiple secure channels to submit Protected Disclosures: 1. **Email:** help@mungiindia.com (secure mailbox monitored by WBO).
2. **Online third-party hotline / web portal:** (vendor to be engaged; see 6A).
3. **In writing:** Sealed envelope addressed to the Whistleblower Officer (marked: "Protected Disclosure – Vigil Mechanism").
4. **Telephone hotline:** [to be provided once vendor selected].
5. **Verbal:** Through immediate manager, HR, or any officer; the receiving official must promptly convert the disclosure to written form and forward to the WBO.

Anonymous reports: Permitted. However, anonymous reports must contain sufficient detail to enable meaningful investigation; anonymous tips lacking detail may not be actionable.

6A. Third-Party Hotline / Portal Implementation

The Company will engage a vendor for an encrypted, 24/7, multilingual reporting hotline/portal. Minimum vendor requirements: encrypted storage, access controls, DPA (Data Processing

Agreement), confidentiality, multilingual support, secure dashboards for the WBO (anonymised data), and the ability to export case logs for internal review. Vendor implementation target: within 90 days of Board approval; hotlines/portal details to be published on intranet and displayed at all sites.

7. What to Report (Scope of Concerns)

Reportable matters include, but are not limited to: - Fraud, theft, embezzlement, or intentional financial irregularities;
- Bribery, corruption, facilitation payments or improper gifts;
- Deliberate violation of law, regulation or Company policy;
- Manipulation, falsification, destruction of records or test data;
- Serious threats to health, safety or the environment;
- Product safety or quality issues that could lead to customer harm or recall;
- Abuse of authority, gross misconduct, conflict of interest;
- Retaliation against anyone for raising a concern in good faith.

Matters that are routine HR disputes, career-related complaints, or grievances that do not raise ethical, legal or safety concerns should be directed to the HR grievance process. Where such matters intersect with wrongdoing, they may be considered under this Policy.

7A. Quality, Safety & Product Integrity (IATF alignment — where applicable)

Where sites or operations are certified under IATF/ISO quality systems, employees and stakeholders are encouraged to report: product defects, test/inspection data manipulation, supplier non-conformance (e.g., counterfeit parts), safety-critical process deviations, and other quality issues. Such reports will be coordinated with the QMS and corrective action processes while ensuring confidentiality.

7B. Environmental, Social & Governance (ESG) Concerns

Reportable ESG issues include major environmental incidents, non-compliance with permits, human rights/labour abuses in supply chain, significant safety failings, discrimination or systemic governance failures.

8. How Reports Are Handled (Intake → Resolution)

1. **Intake & Logging:** WBO logs each report in the secure case management system (or secure register for manual intake) and assigns a unique case ID.

2. **Acknowledgement:** Non-anonymous reporters receive acknowledgement within **7 working days.** Critical cases may receive expedited initial acknowledgement (within 24–48 hours).

3. **Preliminary Assessment / Triage:** WBO conducts a preliminary assessment (target: within **30 calendar days**; see 8A for priority targets) to determine credibility, urgency and

whether interim protective measures are required.

4. **Investigation:** An impartial investigator or Investigation Team (internal and/or external) is appointed. Investigations follow documented procedures: evidence preservation, interviews, documented findings.

5. **Findings & Recommendations:** Investigator submits a written report with findings and recommended corrective actions to the Whistleblower Committee / Audit Committee as per governance.

6. **Decision & Remediation:** Audit Committee / Board or its delegate reviews and approves remedial/discplinary/legal actions.

7. **Feedback to Complainant:** Subject to confidentiality and legal constraints, the reporter will be informed of the outcome in an appropriate form.

8. **Closure & Record Retention:** Case closed with records retained securely (minimum 5 years or as required by law).

8A. Priority-Based Investigation Timeline (Target SLAs)

Timelines below are targets and may be extended with documented justification:

- **Critical (e.g., major fraud, safety emergency, product recall):** Acknowledge within 24–48 hrs; preliminary triage within 5 days; investigation report target 15 days.
- **High (e.g., bribery, significant supplier failure):** Acknowledge within 7 days; triage within 15 days; investigation report target 30 days.
- **Medium:** Acknowledge within 7 days; triage within 30 days; investigation report target 60 days.
- **Low / Non-urgent:** Acknowledge within 7 days; triage within 30 days; investigation report target 90 days.

Complex or cross-border matters may require longer timelines; any extension shall be recorded with reasons and communicated to the Audit Committee.

9. Governance & Roles

- **Whistleblower Officer (WBO):** GM–HR (or nominated officer).
  Responsibilities: receive and log reports, conduct/coordinate triage, ensure confidentiality, manage case logs, coordinate investigators, and prepare anonymised reports to the Audit Committee.

- **Whistleblower Committee / Investigation Team:** Appointed per case; may include HR, Legal, Finance, Compliance and external specialists (as needed) to ensure independence and subject-matter expertise.

- **Audit Committee / Board:** Oversight of Policy implementation; receives anonymised summaries and metrics periodically and reviews significant cases and remedial actions.

- **Escalation:** In exceptional cases (e.g., where the Subject is the WBO or a senior board member), reporters may escalate directly to the Chairperson of the Audit Committee or an independent external reviewer.

9A. Audit Committee Composition & Independence (Where Applicable)

Where applicable under law or the Company's governance framework, the Audit Committee should include independent members and persons with compliance or risk expertise. For private/unlisted entities that do not have independent directors, the Board will appoint suitably senior independent functionaries or external members for oversight of the Vigil Mechanism to ensure impartial review.

9B. Investigator Qualification & Conflict Avoidance

Investigators must be impartial and suitably qualified (experience in compliance, HR investigations, finance or law depending on case nature). Any potential conflict of interest must be disclosed and a recusal recorded. If an internal investigator has a material conflict, an external investigator will be engaged.

10. Confidentiality & Data Protection

All reports, investigations and records are confidential and accessible only to authorised persons on a need-to-know basis. The Company will protect personal data processed in whistleblowing matters using appropriate technical and organisational measures (secure/encrypted storage, access controls, audit logs), and will limit retention to no less than 5 years unless a longer period is required by law or pending litigation.

10A. DPDP & Data Protection Caveat

The Company intends to align processes with relevant data protection laws, including the Digital Personal Data Protection Act (DPDP) and other applicable statutes. Given the evolving regulatory framework for DPDP, the Company will update operational procedures to ensure compliance with finalised rules and guidance. Data Process Agreements and vendor safeguards will be in place for any third-party provider.

11. Protection and Support for Whistleblowers

The Company strictly prohibits retaliation against any person reporting in good faith. Protective measures may include temporary reassignment, access restrictions, paid administrative leave, or other reasonable steps to prevent victimisation during the investigation. Where retaliation is established, the Company will apply corrective actions and remedies as described in Section 11A.

11A. Remedies for Retaliation (Principled Approach)

If retaliation is found, remedies may include reinstatement, restoration of pay and benefits, reversal of adverse actions, counselling, and other appropriate measures. Monetary remedies may be considered on a case-by-case basis and will be approved by the Board in consultation with Legal and HR. This Policy does not create an enforceable entitlement to a fixed monetary amount.

12. False, Vexatious or Malicious Reports

Reports made maliciously or with knowingly false information will be subject to disciplinary action after an objective assessment and following principles of natural justice. However, individuals who report in good faith but whose concerns are not substantiated shall not be subject to disciplinary action.

13. Anonymity & Anonymous Reports

Anonymous reporting is allowed. The ability to investigate anonymous reports depends on the quality and specificity of information provided. The Company encourages reporters to provide contact details to enable follow-up; contact details will be kept confidential.

14. Interim Measures & Confidentiality During Investigation

The Company may implement interim measures (suspension with pay, temporary reassignment, system access restriction, evidence preservation) to protect the integrity of the investigation and safety of parties. All participants (investigators, witnesses, parties) are bound to confidentiality obligations.

15. Record Keeping & Reporting to Board

The WBO will maintain a secure case log and case files containing the complaint, investigation notes, evidence chain-of-custody, findings and actions. A minimum retention period is five (5) years or longer where required by law or litigation hold. The Audit Committee will receive periodic anonymised reports (quarterly or bi-annual depending on Board preference) containing key metrics: number of reports, types of reports, time-to-close, substantiation rate, remedial actions and retaliation findings.

16. Training & Communication

The Policy will be published on the Company website (public summary) and intranet (full policy and contact details). The Company will run awareness sessions and mandatory annual refresher training for all employees. Site-level communication (posters, toolbox talks) will be provided at operational sites.

16A. Implementation & Communication Roadmap (Suggested)

- **Days 1–7:** Board approval and signed resolution; finalise policy and assign WBO.

- **Days 8–30:** Upload policy to intranet/website (public summary), setup secure mailbox, and publish initial communications.
- **Days 31–60:** Conduct targeted awareness & training sessions for leadership and staff; prepare SOPs for investigators.
- **Days 31–90:** Engage and onboard third-party hotline vendor (if approved); print and display hotline details at sites.
- **Month 4+:** Begin periodic reporting and monitoring; annual review cycle initiation.

17. Review & Amendment

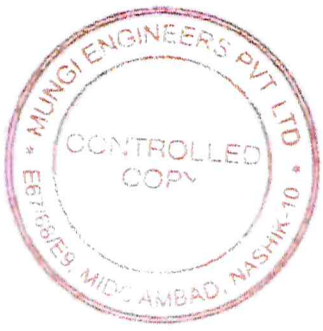
This Policy will be reviewed at least annually or earlier if required by changes in law, regulation, best practice, or business need. The Board reserves the right to amend this Policy; any material changes will be communicated to employees and stakeholders.

18. Miscellaneous

- **Jurisdiction:** The Policy is governed by the laws of India.
- **External Reporting:** Nothing in this Policy prevents any person from reporting concerns to external regulators, law enforcement or other public authorities where permitted or required by law.
- **No Waiver:** Protection in this Policy does not extend to persons who participate in the alleged wrongdoing.

19. Annexures

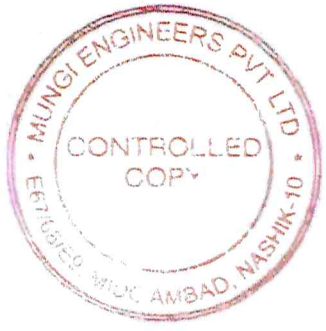
- **Annex A — Reporting Form (Sample)**
- **Annex B — Investigation Checklisy**
- **Annex C — Process Flow (Summary)**
- **Annex D — Plain-Language Quick Reference Guide for Employees**



Board Resolution

Resolved that the Vigil Mechanism (Whistleblower) Policy POL/HR/MEPL-MMC/01, Edition 1.0 (Revision 0) is hereby approved and adopted by the Board of Directors of Mungi Engineers Pvt. Ltd. and Mungi MetalCraft LLP with effect from 13/11/2025, and that the Whistleblower Officer and Compliance team shall implement all provisions and oversee policy communication, reporting and review as per the Policy.

Signature: Vidita Mungi
Name: Vidita Mungi
Title: Director - HR
Date: 13/11/2025



Annex A — Reporting Form (Sample)

A. REPORTER (COMPLETE ONLY IF YOU WISH TO BE CONTACTED)

- Name: _____
- Employee ID (if applicable): _____
- Role / Department / Site: _____
- Work Location (City / Plant): _____
- Contact Number: _____
- Email: _____
- Preferred method for follow-up: ☐ Email ☐ Phone ☐ Do not contact (anonymous)

B. NATURE OF REPORT (tick all that apply)

☐ Fraud / Financial irregularity ☐ Bribery / Corruption ☐ Theft / Asset misuse
☐ Product safety / Quality failure ☐ Safety / Environmental hazard ☐ Data/privacy breach
☐ Harassment / Discrimination (POSH matters handled per POSH policy)
☐ Conflict of interest ☐ Retaliation / Victimisation for prior report
☐ Other (specify): _____

C. INCIDENT DETAILS

1. Date(s) / Time(s) of incident (if known): _____
2. Location(s) / Facility / Department: _____
3. Person(s) involved (Name, Role, Dept — as much as you know):

---

4. Please describe the incident or concern in clear chronological order (what happened, who did what, how you became aware, etc.). Attach extra pages if required:

---

5. Were there any witnesses? ☐ Yes ☐ No
   If Yes — list names/roles and contact info (if known):

---

6. Evidence available (documents, emails, photos, recordings, logs): ☐ Yes ☐ No
   If Yes — describe and attach or indicate location:

---

7. Is there any immediate risk to persons, assets, environment or business continuity? ☐ Yes ☐ No
   If Yes — describe immediate risk: _____

D. ADDITIONAL INFORMATION / SUGGESTED ACTION (optional)

E. DECLARATION (to be signed if non-anonymous)

I confirm that, to the best of my knowledge and belief, the information provided in this report is true and correct. I understand that malicious or deliberately false allegations may be subject to disciplinary action. I also understand that the Company will protect my identity as far as possible and will not tolerate retaliation for good-faith reports.

Signature: _____ Name (printed): _____
Date: ____ / ____ / _____

F. FOR OFFICIAL USE ONLY (WBO / INVESTIGATOR)

- Case ID: _____
- Date Received: ____ / ____ / _____ Mode of receipt: ☐ Email ☐ Letter ☐ Hotline ☐ In-person ☐ Other: _____
- Acknowledgement sent to reporter (if non-anonymous): ☐ Yes ☐ No Date: ____ / ____ / _____
- Initial risk rating: ☐ Critical ☐ High ☐ Medium ☐ Low
- Assigned investigator(s): _____

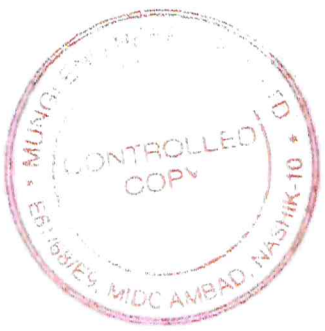
- Investigation start date: ____ / ____ / _____ Target completion date: ____ / ____ / _____
- Evidence logged (files / refs): _____
- Interim protective measures taken (if any): _____
- Summary of preliminary findings / assessment: _____

- Final report submitted to: ☐ Audit Committee ☐ Board ☐ CEO ☐ Legal ☐ Other: _____ Date submitted: ____ / ____ / _____
- Final outcome / action taken (disciplinary / remedial / other):

- Case closed date: ____ / ____ / _____ File retention location / ref: _____

PRIVACY & CONFIDENTIALITY NOTE

All information submitted will be treated confidentially and disclosed only on a strict need-to-know basis for investigation. The Company will store records securely and retain them for a minimum of **5 years** or longer if legally required. If you provided contact details, the Whistleblower Officer may contact you for clarification — communications will respect confidentiality.



Annex B — Investigation Checklist (Sample)

1. Log & acknowledge receipt; assign case ID.Conduct preliminary triage and preservation of evidence.
2. Appoint investigator(s) and document scope.
3. Interview complainant, subject, witnesses; maintain interview notes.
4. Collect and secure documentary, system and physical evidence (chain of custody).
5. Prepare draft findings and seek legal review (if required).
6. Finalise report and present to Whistleblower Committee / Audit Committee.
7. Implement corrective/remedial actions and monitor.
8. Close case and archive documentation securely for retention period.

Annex C — Process Flow (Summary)

Report received → Log & Acknowledge → Triage → Investigation → Findings & Recommendations → Governance Decision → Remediation → Feedback & Closure → Record retention

---

Annex D — Plain-Language Quick Reference (For Employees)

Why use this? To report suspected wrongdoing safely and confidentially.
Who can report? Employees, contractors, suppliers, customers, shareholders.
What to report? Fraud, bribery, safety, environment, product issues, retaliation, serious misconduct.
How to report? Email help@mungiindia.com, hotline/web portal, sealed letter, or via HR/manager.
Can I be anonymous? Yes — but provide detail so we can investigate.
Will I be protected? Yes — no retaliation for good faith reporting.
What happens next? We acknowledge, assess, investigate, take action, and inform you of outcome within confidentiality limits.

Document control:
Policy owner: Whistleblower Officer (GM–HR)
Version history:- 1.0 — [13/11/2025] — Original

MUNGI ENGINEERS PVT LTD
CONTROLLED COPY
E67/68/E9, MIDC AMBAD, NASHIK-10