WHISTLE BLOWER POLICY

Document Control Section

Version	Release Date	Summary of Changes Made	Reviewed By	Approved By
1.0	1st August 2021	New Policy Roll Out	CFO | Head HR | Head – Strategy (MD's Office) | CEO – Fund Management	Introduction of policy
1.1	1st September 2022	Changed Chief Ethics Officer	Jonathan D'Souza CHRO – Welspun One	NA – Standard Change
1.2	23rd November 2022	Changed Chief Ethics Officer	Jonathan D'Souza CHRO – Welspun One	Harishchandra Gupta Welspun Group
1.3	15th March 2023	Updated Procedure for reporting & dealing with disclosures on page 6	Harish Kesharwani Chief Ethics Officer Jonathan D'Souza CHRO – Welspun One	Harishchandra Gupta Welspun Group
1.4	9th September 2024	1. Changed company name from Welspun One Logistics Parks to Welspun One Pvt. Ltd. 2. Changed Chairman to Chairperson	Jonathan D'Souza CHRO – Welspun One	NA
1.5	31st March 2025	1. Exceptional Cases – Define cases for direct Chairperson access. 2. Business Hold – Prevent email deletion/alteration. 3. Case Reference Number – Assign for all disclosures. 4. Former Employees – Extend policy coverage.	Mekhola Ganguly HRBP – Welspun One Sachin Shinde CRO – Welspun One	Jonathan D'Souza CHRO – Welspun One

		5. Fraud Response Plan – Reference for investigations. **6. Terminology – Standardize "Ethics Officer" usage.** **7. Typo Correction – Fix redundancy on page 11.** **8. Examples – Clarify improper practices.** **9. Policy Updates – Define stakeholder notification process.** **Changed by Susan Chouri** **HR Manager – Welspun One**		

TABLE OF CONTENTS

WHISTLEBLOWER POLICY

1. OBJECTIVE

Welspun One Pvt. Ltd. ("Company") is committed to adhere to the highest standards of ethical, moral and legal conduct of business operations. The Company had adopted Code of Conduct - Whistle blower policy which lays down the principles that govern the actions of the Company, its employees and its stakeholders. To maintain these standards, the Company encourages its employees and stakeholders who have concerns about any actual or potential violation, legal & regulatory requirements, incorrect or misrepresentation of any financial statements and reports, etc. any claim of theft or fraud, and any claim of retaliation for providing information to or otherwise assisting the Chief Ethics Officer or the Ethics Committee for investigation , to come forward and express his/her concerns without fear of punishment or unfair treatment.

This Policy aims to provide an avenue for employees, directors and stakeholders to raise their concerns that could have grave impact on the operations, performance, value and the reputation of the Company to approach the Chief Ethics Officer and Ethics Committee of the Company. It also empowers the Ethics Committee of the Board of Directors to investigate the concerns raised by the employees, directors and stakeholders.

2. DEFINITIONS

"Company" means, "Welspun One Pvt. Ltd." and all its subsidiaries as defined under the Companies Act, 2013 as amended from time to time

"**Chief Ethics Officer or Ethics Officer**" means the Employee designated as Chief Ethics Officer of the Company.

"**Disciplinary Action**" means, any action that can be taken on the completion of /during the investigation proceedings as per disciplinary action matrix implemented by the Company.

"**Disciplinary Action Committee**" means the committee constituted by the Company from time to time comprising of select senior employees of the Company.

"**Ethics Committee**" means the committee constituted by the Company from time to time comprising of select senior employees of the Company and Chief Ethics Officer

"**Employee**" means, every employee of the Company (whether working in India or abroad) including the Directors in the employment of the Company.

"**Fact Finder**" shall mean, the person(s) or outside entity appointed by the Chief Ethic's officer/ Ethics Committee to investigate a Protected Disclosure.

"Good Faith": A whistleblower shall be deemed to be communicating in "good faith" if there is a reasonable basis for communication of unethical and Improper Practices or any other alleged wrongful conduct. Good Faith shall be deemed lacking when the whistleblower does not have personal knowledge on a factual basis for the communication or where the whistleblower knew or reasonably should have known that the communication about the unethical and Improper Practices or alleged wrongful conduct is malicious, false or frivolous.

"**Improper Practice**" includes but not limited to :

a) Any actual or potential violation of the legal & regulatory requirements whether Criminal/ Civil;
b) Any claim of theft or fraud;
c) Bribery, corruption and kickback;
d) Abuse of authority;
e) Conflict of interest;
f) Breach of contract/ trust, pilferation of confidential/propriety information;
g) Negligence causing substantial and specific danger to public health and safety;
h) Manipulation/ theft of the Company data/records;
i) Financial irregularities, including fraud or suspected fraud or deficiencies in Internal Control and check or deliberate error in preparations of Financial Statements or Misrepresentation of financial reports;
j) Wastage/misappropriation of the Company funds/assets, embezzlement;
k) Concurrent/Dual employment;
l) False expense reimbursement;
m) Unfair trade practices and anti-competitive behavior;
n) Instances of leakage or suspected leakage of unpublished price sensitive information;
o) Breach of Company Policy or failure to implement or comply with any approved Company Policy/ies;
p) Any claim of retaliation for providing information to or otherwise assisting the Ethics Committee;
q) Any other action or inaction that could have significant impact on the operations, performance, value and the reputation of the Company.

"**Policy or "This Policy"** means, the "Whistleblower Policy."

"**Protected Disclosure**" means, any communication made in good faith that discloses or demonstrates information that may evidence Improper Practice. Protected Disclosures should be factual and not speculative in nature.

"Stakeholders" means and includes directors, employees, former employees, vendors, any third parties, suppliers, lenders, customers, business associates, trainees, interns, and any others with whom the Company has any financial or commercial dealings.

"**Subject**" means, a person or group of persons against or in relation to whom a Protected Disclosure is made or evidence gathered during the course of an investigation under this Policy.

"**Whistleblower**" is someone who makes a Protected Disclosure under this Policy or voluntarily provides information under the Securities and Exchange Board of India (Prohibition of Insider Trading) Regulation, 2015 as amended from time to time. The whistle blower may disclose his/her identity or choose to remain anonymous while reporting any Protected Disclosure.

"Voluntarily providing information" means, providing the Securities and Exchange Board of India, with information before receiving any request, inquiry, or demand from the Securities and Exchange Board of India, any other Central or State authorities or other statutory authority about a matter, to which the information is relevant.

3. SCOPE

Various stakeholders of the Company are eligible to make Protected Disclosures under the Policy. These stakeholders may fall into any of the following broad categories:

- Employees of the Company;
- Trainees and contractual employees of the Company;
- Employees of other agencies deployed for the Company's activities, whether working from any of the Company's offices or any other location;
- Existing / Prospective Contractors, vendors, suppliers or agencies (or any of their employees) providing any material or service to the Company;
- Customers, bankers of the Company;
- Any other person having an association with the Company.

A person belonging to any of the above-mentioned categories can avail of the channel provided by this Policy for raising an issue covered under this Policy.

The Policy should not be used for routine or operational matters for which separate grievance mechanism exist. For. e.g.

- Strategic and management related decisions;
- Improper / inappropriate administration facilities;
- Malfunctioning of IT assets (laptops, printers, etc.);
- Compensation related issues;
- Payment and taxation related queries;
- HR related matters e.g. transfers, relocation, promotion, demotion, growth related issues etc.;
- Raising malicious or unfounded allegations against colleagues;
- Allegations related to Sexual Harassment;
- Incidences covered under the any other Grievance Handling mechanism.

4. ANONYMOUS DISCLOSURES

This Policy encourages individuals to put their name to any Protected Disclosures they make. Protected Disclosures expressed anonymously may be considered at the discretion of the Chief Ethics Officer/Ethics Committee. In exercising this discretion, the factors to be considered will include:

i. The seriousness of the issues raised;
ii. The credibility of the concern;
iii. The likelihood of confirming the allegation from attributable sources;
iv. The ability to investigate into anonymous complaints.

5. PROCEDURE FOR REPORTING & DEALING WITH DISCLOSURES

A. Following channels are available for making Protected Disclosures:

1. Third Party Ethics Helpline:

The Company had appointed an independent third party to facilitate reporting of Protected Disclosures through a toll-free helpline number. The toll-free number is available with option to communicate in languages, as set out below:

Telephone Number	Languages
000 800 919 0236	English, Hindi

These toll-free numbers can be accessed 24 hours a day, seven days a week.

2. A Protected Disclosure can be made in writing by an email or by Post to the Chief Ethics Officer of the Company. The details are as under:

   Chief Ethics Officer
   Postal Address: Harish Kesharwani, 7th Floor, Welspun House, Kamala Mills Compound, Lower Parel, Mumbai - 400013
   Email id: whistleblower_wolp@welspun.com

   You can also drop an anonymous complain on our website www.Welspun.ethicspoints.com

3. A Protected Disclosure can also be made over email to the Chairperson of the Ethics Committee in exceptional cases divya_verma@welspun.com

   If a Protected Disclosure is received by any employee including senior management / Director of the Company other than Chairperson of Ethics Committee or the Chief Ethics Officer, the same should be forwarded to the Company's Chief Ethics Officer for further appropriate action. Appropriate care must be taken to keep the identity of the Whistleblower confidential.

   Exceptional Cases would mean the following -

   a) Protected Disclosures which are serious in nature such as Protected Disclosures against CEO / CFO / VP-Finance/COO / KMP/ CRO or any other member of the Senior Management team of the Company.

   b) Protected Disclosures against any Director or Chairman of the Company or Protected Disclosures against the Compliance Officer.

   If an employee observe any ethical violation, he/she should report through any of the channels mentioned above.
4. For every Protected Disclosure made through any of the reporting channels, a case reference number will be provided to the Whistleblower, which can be used for further communication like providing additional information or knowing the status of the complaint.

B. Is there any specific format for submitting the Protected Disclosure?

While there is no specific format for submitting a Protected Disclosure, the following details must be mentioned wherever possible:

In case of postal letter, the Protected Disclosure should be sealed in an envelope marked "Confidential" and addressed to the Chief Ethics Officer

i. In case of e-mail, the Protected Disclosure should be marked "Confidential" and the subject line should contain "Whistleblower Complaint" and addressed to the email id of Chief Ethics Officer

ii. Name, address and contact details of the Whistleblower if he/she chooses to disclose.

iii. The Complaint should provide the following details

- The employee, and/or outside party or parties involved;
- The Company and the business area where it happened (Location, Department, Office);
- When did it happen: a date or time;
- Amount involved
- Nature and detailed fact of the Improper Practice;
- Evidence to support the allegations made;
- Details of any witnesses or those who can corroborate the allegations;

C. What will happen after the Protected Disclosure is submitted?

i. The Ethics Officer shall acknowledge receipt of the Protected Disclosure as soon as practical (preferably within 20 days of receipt of a Protected Disclosure), where the Whistleblower has provided his/her contact details.

ii. The Chief Ethics Officer will conduct a preliminary enquiry of the Protected Disclosure received under this Policy. If, based on preliminary enquiry, it appears that the complaint reported has no basis, or it is not a matter to be pursued under this Policy, it may be dismissed at that stage and the decision is documented in consultation with the Ethics Committee.

iii. If required, the Chief Ethics Officer can appoint Fact Finder to conduct an investigation in consultation with the Ethics Committee. The Ethics Committee will decide on the need for investigation based on the preliminary enquiry.

iv. If any of the members of the Ethics Committee have a conflict of interest in a given case, such person/s will recuse themselves and the other members on the Committee would deal with the matter on hand.

v. If the alleged Improper Practice is required by law to be dealt with under any other mechanism, the Chief Ethics Officer in consultation with Ethics Committee shall refer the Protected Disclosure to the appropriate authority under such mandated mechanism and seek a report on the findings from such authority.

vi. Subjects may be informed of the allegations at the outset of a formal investigation and have opportunities for providing their inputs during the investigation. Subject may be informed of the outcome of the inquiry/ investigation process.

vii. The identity of a Subject will be kept confidential to the extent possible given the legitimate needs of law and the investigation.

viii. Subject shall have a duty to co-operate during the investigation to the extent that such co-operation will not compromise self-incrimination protections available under the applicable laws.

ix. The investigation may involve study of documents and interviews with various individuals. Any person required to provide documents, access to systems and other information to the Chief Ethics Officer for the purpose of such investigation shall do so. Individuals with whom the Chief Ethics 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.

x. The Chief Ethics Officer shall conduct the investigations in a timely manner and shall submit a written report containing the findings with the Ethics Committee. The Ethics Committee can recommend action to be taken as per disciplinary action matrix to the Disciplinary Action Committee.

xi. If the Improper Practice constitutes a criminal offence, the Ethics Committee will bring it to the notice of the Managing Director after consultation with the Legal department and take appropriate action.

xii. An employee or other stakeholder who knowingly makes false allegations shall be subject to disciplinary action, up to and including termination of employment, removal from the office of directorship or termination of contract in case of other stakeholder in accordance with Company rules, policies and procedures.

D. Business Hold

a. The "Business Hold" feature shall be configured to prevent any deletion or alteration of emails within the account, thereby preserving all received whistleblower communications as potential evidence for any subsequent investigations or inquiries.

b. The IT department is responsible for the activation, maintenance, and regular verification of the "Business Hold" feature to ensure its effective operation.

c. Any attempt to disable or bypass the "Business Hold" feature without proper authorization from the Board, will be considered a violation of this policy and may result in disciplinary action, up to and including termination of employment.

6. PROTECTION TO WHISTLEBLOWER:

a) The identity of the Whistleblower shall be kept confidential to the extent possible and permitted under law. If a Whistleblower raises a concern under this Policy or voluntarily providing information under the Securities and Exchange Board of India (Prohibition of Insider Trading) Regulations, 2015, he/she will not be at risk of suffering any form of reprisal or retaliation. Retaliation includes discrimination, reprisal, harassment or vengeance in any manner, risk of losing his/her job or suffer loss in any other manner like transfer, demotion, refusal of promotion, or the like including any direct or indirect use of authority to obstruct the Whistleblower's right to continue to perform his/her duties/functions including making further Protected Disclosure, as a result of reporting under this Policy. The protection is available provided that:

i. the communication/ disclosure is made in good faith;
ii. the Whistleblower reasonably believes that information, and any allegations contained in it, are substantially true; and
iii. the Whistleblower is not acting for personal gain,

Anyone who abuses the procedure (for example by maliciously raising a concern knowing it to be untrue) will be subject to disciplinary action, as will anyone who victimizes a colleague by raising a concern through this

procedure. If considered appropriate or necessary, suitable legal actions may also be taken against such individuals.

However, no action will be taken against anyone who makes an allegation in good faith, reasonably believing it to be true, even if the allegation is not subsequently confirmed by the investigation.

b) The Company will not tolerate the harassment or victimization of anyone raising a genuine concern. As a matter of general deterrence, the Company may publicly inform employees of the penalty imposed and discipline of any person for misconduct arising from retaliation. Any investigation into allegations of potential misconduct will not influence or be influenced by any disciplinary or redundancy procedures already taking place concerning an employee reporting a matter under this Policy.

c) Any other employee or stakeholder assisting in the said investigation shall also be protected to the same extent as the Whistleblower.

d) If a Whistleblower faces any retaliatory action or threats of retaliatory action as a result of making a Protected Disclosure, he/she can report the matter to the Chairperson of Ethics Committee in writing immediately to the email id mentioned in Section 5 above. The Chairperson of the Ethics Committee will treat reports of such actions or threats as a separate Protected Disclosure and investigate the same accordingly and may also recommend appropriate steps to protect the Whistleblower from exposure to such retaliatory action and ensure implementation of such steps for the Whistleblower's protection.

7. ESCALATION PROTOCOL

The Chief Ethics Officer shall inform the Whistleblower about the closure of the case where the contact details are provided. In case a Whistleblower is not satisfied with the closure of Protected Disclosure submitted, then he/she may write to the Chairperson of the Ethics Committee with details of his/her Protected Disclosure and reason for dissatisfaction. The Chairperson of the Ethics Committee will take appropriate steps after consultation (if required) with the other members of the Ethics Committee. The decision of the Ethics Committee shall be final for such cases.

8. REPORTING

A quarterly report on the total number of Protected Disclosures received during the period, with summary of the findings of the investigation and the corrective actions taken will be reported by Chief Ethics Officer to the Ethics committee. The Ethics Committee would submit to the Board of the Company.

ACTION GRID WITH TIMELINES FOR INVESTIGATION

a) The timeline for completion of preliminary review and detailed investigation is mentioned below:

<table>
<tr><th>Priority</th><th>Preliminary review</th><th>Completion of Investigation</th><th>Disciplinary Action</th></tr>
<tr><td>Priority 1</td><td rowspan="4">Chief Ethics Officer to perform preliminary review to verify the facts and genuineness of the complaint within 7 working days of its receipt.</td><td>20 working days from the date of receipt of complaint</td><td rowspan="4">The Ethics Committee shall recommend to the Management of the Company to take Disciplinary Action based on the guidelines mentioned in the Disciplinary Action Matrix of the Company</td></tr>
<tr><td>Priority 2</td><td>25 working days from the date of receipt of complaint</td></tr>
<tr><td>Priority 3</td><td>35 working days from the date of receipt of complaint</td></tr>
<tr><td>Priority 4</td><td>45 working days from the date of receipt of complaint</td></tr>
</table>

Note – For minimum attributes of investigation report, retention period, duties and responsibilities of Ethics Committee and Chief Ethics Officer - Refer to the Fraud Response Plan of the Company

9. GUIDANCE ON INVESTIGATION

I. PROTECTION AND NON-RETALIATION

a) The identity of the Whistleblower shall be kept confidential to the extent possible and permitted under law.

b) If a Whistleblower raises a concern under the Whistle Blower Policy, he/she will not be at risk of suffering any form of reprisal or retaliation. Retaliation

includes discrimination, reprisal, harassment or vengeance in any manner, risk of losing her/ his job or suffer loss in any other manner like transfer, demotion, refusal of promotion, or the like including any direct or indirect use of authority to obstruct the Whistleblower's right to continue to perform his/her duties/functions including reporting further complaints the Whistle Blower Policy.

II. PLANNING AND STRATEGY

a) The Chief Ethics Officer/investigating team should properly plan and strategize the procedures of an investigation.

b) The internal and external communication protocols should be clearly established.

c) The Chief Ethics Officer should review and provide guidance to investigating team in relation to compliance with all the regulatory requirements during the course of the investigation.

III. PROCEDURES

a) Investigative procedures may include the following:

i. Review of documents available in the human resource file of the Subject(s);
ii. Interview of the Subject(s), other employees, third party etc.;
iii. Review of documentary and electronic evidence;
iv. Forensic Computer Imaging (should be done by certified professionals only).
v. Desktop and database searches;
vi. Conducting background checks;
vii. Field work, if required;
viii. Any other procedures deemed necessary based on the facts available for the case under review.

b) Consider seeking legal and expert opinion whenever required.

c) Do not confront suspected employee or third party without appropriate evidence.

d) Always respect the rights of an individual.

e) Provide 'equal opportunity of being heard' to all.

f) Maintain highest level of confidentiality

g) Maintain a record of all events – meetings, site visits, telephone calls, etc.

h) Consider usage of appropriate headers in communication like "Strictly Confidential" or "Private and Confidential".

10. ACCESS TO REPORTS AND DOCUMENTS

All reports and records associated with the "Protected Disclosures" are considered confidential information and access will be restricted to Chief Ethics Officer and the Ethics Committee. "Protected Disclosures" and any resulting investigations, reports or resulting actions will not be disclosed except as required by any legal requirements or regulations.

All Protected Disclosures in writing or documented along with the results of investigation relating thereto shall be retained by the Company for a minimum period of 5 years.

11. GUIDING PRINCIPLES

To ensure that this Policy is adhered to, and to assure that the concern will be acted upon seriously, the Company will:

a) Ensure that the Whistleblower and/or the person processing the Protected Disclosure are not victimized for doing so. But this does not extend to immunity for involvement in the matters that are the subject of the allegations and investigation.
b) Treat victimization as a serious matter, including initiating disciplinary action on such person/(s).
c) Ensure confidentiality.
d) Not attempt to conceal evidence of the Protected Disclosure.
e) Take disciplinary action, if any one destroys or conceals evidence of the Protected Disclosure made/to be made.
f) Provide an opportunity of being heard to the persons involved especially to the Subject.
g) Ensure that this Policy may not be used as a defense by an employee against whom an adverse action has been taken independent of any disclosure of intimation by him/her and for legitimate reasons or cause under Company rules and policies.

12. COMPANY'S POWERS

The Board of Directors of the Company may subject to applicable laws and at the recommendation of the Ethics Committee is entitled to amend, suspend or rescind this Policy at any time. Any difficulties or ambiguities in the Policy will be resolved by Ethics Committee in line with the broad intent of the Policy and in consultation with the Ethics Committee. The Ethics Committee may also establish further rules and procedures, from time to time, to give effect to the intent of this Policy and further the objective of good corporate governance.

13. ILLUSTRATIVE LIST OF IMPROPER PRACTICES

- **Theft** – "The act of stealing data, property, or funds belonging to the company."

- **Fraud** – "Any act of deception, misrepresentation, or falsification of records intended to gain an unfair advantage, including financial fraud, expense report falsification, or misrepresentation of company data."

- **Bribery & Corruption** – "Offering, giving, receiving, or soliciting anything of value (such as cash, gifts, or favors) to improperly influence a business decision or gain an unfair advantage."

- **Conflict of Interest** – "Engaging in activities or relationships that compromise or appear to compromise an individual's ability to act in the best interests of the company, such as personal financial dealings with vendors or competitors."

- **Insider Trading** – "Using confidential or non-public information about the company to trade stocks or securities for personal gain or sharing such information with others for financial benefits."

- **Data Breach & Confidentiality Violation** – "Unauthorized access, disclosure, or misuse of sensitive company information, including customer data, trade secrets, or employee records."

- **Harassment & Discrimination** – "Any unwelcome conduct, verbal or physical, that creates a hostile work environment based on race, gender, religion, nationality, or other protected characteristics."

- **Misuse of Company Resources** – "Using company property, funds, or digital assets for personal gain, including unauthorized use of corporate credit cards, company vehicles, or IT systems."

- **Falsification of Records** – "Manipulating or altering official company documents, reports, or time records to mislead management, auditors, or regulators."

- **Non-Compliance with Legal & Regulatory Requirements** – "Failing to adhere to laws, industry regulations, or company policies that could result in legal penalties or reputational damage."

- **Retaliation against Whistleblowers** – "Taking adverse action against an employee or stakeholder for reporting ethical violations, misconduct, or fraud in good faith."

- **Nepotism & Favoritism** – "Unfairly giving preferential treatment in hiring, promotions, or other business decisions based on personal relationships rather than merit or qualifications."

- **Embezzlement** – "The unauthorized appropriation of company funds or assets for personal use, such as misdirecting company payments or manipulating financial records for personal gain."

- **Kickbacks & Illegal Commissions** – "Receiving or offering undue benefits, payments, or commissions to influence business decisions, including supplier or vendor selection."

- **Workplace Violence & Threats** – "Any act of physical aggression, intimidation, or threats towards employees, customers, or business associates that creates a hostile or unsafe work environment."

- **Substance Abuse in the Workplace** – "The use, possession, or distribution of illegal drugs or alcohol on company premises or during work hours, impairing productivity and workplace safety."

- **Cybersecurity Violations** – "Deliberately compromising the security of company systems, including unauthorized access to IT infrastructure, phishing attacks, or intentional data leaks."

- **Sabotage** – "Intentionally damaging, destroying, or obstructing company operations, including tampering with equipment, software, or company assets."

- **Plagiarism & Intellectual Property Theft** – "Copying, misrepresenting, or unauthorized use of company intellectual property, trademarks, or copyrighted materials without permission."

- **Non-Disclosure & Breach of Confidentiality Agreements** – "Failing to maintain the confidentiality of trade secrets, business strategies, or proprietary information, leading to competitive disadvantage or legal risks."

- **Non-Adherence to Workplace Safety Norms** – "Violating safety protocols, failing to use protective equipment, or engaging in reckless behavior that endangers oneself or others at the workplace."

- **Time Theft** – "Engaging in activities such as falsifying attendance records, excessive personal time on company resources, or intentionally underperforming while on duty."

- **False** C**laims & Misrepresentation** – "Providing misleading or exaggerated information in reports, project updates, or marketing materials to deceive stakeholders or gain an undue advantage."

- **Unethical** C**ompetitive Practices** – "Engaging in anti-competitive behavior, price-fixing, or unauthorized access to competitor data to manipulate the market unfairly."

- **Misuse of Position or Authority** – "Abusing one's role to gain personal benefits, influence decisions improperly, or intimidate subordinates for personal or financial gain."

- **Non-Cooperation in Investigations** – "Withholding information, misleading investigators, or obstructing internal or external audits, compliance checks, or legal inquiries."

Note – The above list is illustrative and not exhaustive in nature.

Note - Policy Communication & Accessibility

Any amendments to this policy shall be communicated to all employees via email within seven (7) days of the amendment, along with a copy of the updated policy.

Additionally, the amended policy shall be uploaded on the company's intranet and/or website within seven (7) days from the date of amendment to ensure accessibility for all stakeholders.