

Confidentiality policy

Introduction:

Resurgent ESG Services Pvt. Ltd. ("Resurgent ESG") attaches utmost importance to confidentiality in all aspects of its business operations. Our competitive advantage, the level of trust with clients, and compliance with applicable legal and regulatory obligations all rely on the protection of non-public information. This policy describes how employees, subcontractors, and associated parties shall treat and protect confidential information.

Policy Objective:

- To ensure that all information created, received, and owned by Resurgent ESG is kept confidential.
- To distinctly identify the categorization with regard to the handling, storage, and disclosure of personal information.
- Ensure compliance with all related and applicable laws and regulations concerning privacy and the protection of data.
- Foster an environment of responsibility and integrity in handling sensitive information.

3. Scope and Applicability

The policy applies to all employees, be they temporary, full-time, or part-time staff; contractors; consultants; and any other third party that may have access to private data belonging to Resurgent ESG. The policy encompasses all types of sensitive information, including information communicated or maintained in written, spoken, electronic, and other media.

4. Definition of Confidential Information

For the purpose of this Policy, Confidential Information at Resurgent ESG shall include, but is not limited to:

- **Business Information:** This includes strategic plans, financial projections, business processes, and generally any information on business operations not publicly disclosed.
- **Client Information:** All data, reports, and communications pertaining to clients, including but not limited to contract information, client preferences, and sensitive business information provided by the clients.
- **Intellectual Property:** Anything to do with proprietary methodologies, research data, software codes, algorithms, and generally innovations developed by or for Resurgent ESG.
- **Employee Information:** Employee personal information such as, but not limited to, salaries, benefits, performance reviews, and personnel records.
- **Trade Secrets:** Proprietary methodologies, systems, and technologies offering Resurgent ESG an advantage over their competitors.
- **Non-Public Financial Information:** Financial statements, budgets, forecasts, or any other financial information internally prepared that has not been publicly disclosed.

RESURGENT ESG SERVICES PRIVATE LIMITED

Corporate Identification Number- U74900HR2024PTC120292

Unit No. 904, 9th Floor, Tower - C, Unitech Business Zone,

Nirvana Country, South City - II, Sector - 50, Gurgaon – 122018

Phone: +91 880045 3356, Email: enquiry@resurgentesgratings.com

5. Employee Responsibilities

Resurgent ESG employees must ensure information confidentiality. This is guaranteed through the following ways:

5.1 Commitment to Confidentiality: Employees of Resurgent ESG acknowledge and agree to the confidentiality obligations outlined in the appointment letter, ensuring the protection of all sensitive company information during and after their tenure.

5.2 Access Control: Access to information classified as confidential is strictly on a need-to-know basis. Employees have access to confidential information required for performance of their job functions but should not attempt to access other information that is not related to their area of work.

5.3 Information Handling:

Physical Security: Documents containing any confidential information must be physically stored in secure, locked environments. Desks must be cleaned at the end of the day and all papers not left unattended.

Digital Security: Passwords used must be strong. No confidential information is to be kept or stored on personal devices or across unsecured networks.

Communication: All discussions regarding confidential matters should be conducted in a secured environment.

5.4 Internal Sharing: When confidential information is shared within Resurgent ESG, this should be appropriately restricted, allowing access only to individuals who have a need to know in order to fulfill their job duties. Information should be reminded as being of a confidential nature.

5.5 External Communication: No employee shall disclose confidential information to any external party, including family, friends, or business contacts without prior explicit authorization by Resurgent ESG, or as so required by law. Disclosure in such cases should be restricted to the need-to-know principle.

5.6 Protection of Customer Data: Customer information is highly sensitive. The employees will be bound to follow any particular agreement on confidentiality with each customer and handle the information due to care.

5.7 Retention and Disposal: The confidential information shall be retained only for such period as may be necessary to satisfy the business purpose or such statutory requirements as may apply. The documents containing physical confidential information shall be shredded and in case of a digital file, delete the same through secured mode of deletion.

5.8 social media and Public Statements: No employee should disclose or share any information that is of a confidential nature on social media or in open forums. Such information leading to the indirect disclosure of sensitive data falls within this ambit.

6. Incident Reporting and Breach Management

6.1 Reporting Suspected Breaches: Any suspected or actual breach of confidence shall be immediately reported to the compliance officer or immediate supervisor. The sooner such an incident is reported, the less potential damage there is likely to be.

6.2 Investigation and Response: All reported breaches shall be investigated. When a breach is confirmed, appropriate action shall be taken by Resurgent ESG, including disciplinary measures, legal action, and measures to prevent future breaches.

6.3 Corrective Action: After any breach, Resurgent ESG shall institute corrective action, which may also include updating the security protocols, giving additional training, or updating the policy on confidentiality.

7. Legal and Compliance

Resurgent ESG dedicates its efforts to the adherence to all applicable legislation and regulations on confidentiality and protection of data. In this line, Resurgent ESG would mean that it shall:

8. Training and Awareness

8.1 Training: All staff members shall be subjected to training in matters relating to confidentiality, data protection, and handling of information securely. Refresher courses shall be conducted annually.

8.2 Awareness Campaigns: Awareness campaigns shall be done on a periodic basis to remind the staff about their responsibilities under this policy as well as to update them concerning any changes or amendments.

8.3 Confidentiality Acknowledgment: Staff members shall periodically confirm their awareness of this policy and confirm their commitment to maintaining confidentiality.

9. Compliance and Sanctions

Breaches of this policy will be treated seriously and are subject, amongst others, to:

- Disciplinary action up to and including termination.
- Legal action where necessary to seek damages or injunctive relief to prevent further unauthorized disclosures.
- Reporting of the incident to relevant regulatory body in case it is obliged to do so under law.

10. Policy Review and Amendments

This policy will be reviewed yearly and updated in case of any change in law, regulations, or operations affecting the company. Changes will be relayed to all employees, with continued adherence being mandated.