CYBER SECURITY POLICY

Gujarat Fluorochemicals Limited and its subsidiaries together referred to herein after as "the Company", endeavour to ensure and maintain the privacy and security of personal information, if any, collected or retrieved by GFL on account of your visit to our Website www.gfl.co.in, for viewing or download of any information pertaining to GFL.

We pledge to comply with the recognised standards of privacy protection and meet the requirements prescribed under the following Act and Rule:

- The Information Technology Act, 2000 – Section 43A
- The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011.

The company recognises the importance of cyber security and data privacy in ensuring sustainable growth and business continuity across the organisation. Information systems and data resources of the company are critically important assets for its business operations and effective customer services.

Policy Commitments:

- To comply with the applicable national and international cyber security standards.
- Establishing and improving cyber security preparedness and minimising its exposure to associated risks to safeguard the company's assets.
- Critical information is protected from unauthorised access, use, disclosure, modification and disposal, whether intentional or unintentional.
- The confidentiality, integrity and availability of critical information acquired permanently or in transit, provided or created are always ensured.
- To conduct regular cybersecurity audits following appropriate national and international standards to maintain compliance.
- To communicate the importance of cyber security and to continually enhance information security capabilities.
- To protect the company's stakeholders, information and assets from threats that could potentially disrupt business and Adani brand and reputation.
- All Business Heads/Department Heads are directly responsible for ensuring compliance with this policy in their respective business domains.
- To collaborate with cyber security experts to continually upgrade the information management infrastructure.
- Establishing information security requirements for employees and third parties not limited to suppliers, contractors and other relevant stakeholders.
- All breaches of information security, actual or suspected, are reported, investigated by the designated personnel and appropriate corrective and preventive actions initiated.
- This policy shall be reviewed periodically for its suitability and updated, as necessary.

This policy applies to full time employees (FTE) and off-roll employees, including but not limited to subsidiary staff, contractors, consultants, interns, temporary staff affiliated with third parties, including system vendors and staff from outsourcing companies.