TRIVENI ENGINEERING AND INDUSTRIES LTD
CYBER SECURITY AND DATA PRIVACY POLICY

Background/Preamble:

Triveni Engineering and Industries Limited (hereinafter referred to as 'the Company' and 'TEIL') recognizes the importance of cyber security and data privacy in ensuring sustainable growth and business continuity across the organization. Information systems and data resources of TEIL are critically important assets for its business operations and effective supply chain and customer services.

TEIL is committed in establishing and improving cyber security preparedness and minimizing its exposure to associated risks to safeguard TEIL assets. All TEIL businesses and functions implement adequate security policies, processes, and controls to protect confidentiality, maintain integrity, and ensure availability of all information assets.

Purpose and Scope:

This Policy outlines the measures and procedures that the Company has implemented to protect its data and information systems from cyber threats. The policy applies to all employees or any external person who may have access or use the company's information systems and data.

Commitment:

This policy requires all Businesses under TEIL:

1. To comply with the applicable national cyber security standards.
2. For implementation of control and monitoring measures for all hardware and software assets in use throughout the organization
3. For implementation of management protocols for protection and security of stakeholders' assets in identifying the risks to information and cyber systems
4. To ensure that the critical information is protected from unauthorized access, use, disclosure, modification, and disposal, whether intentional or unintentional
5. (i) To ensure the confidentiality, integrity and availability of such information acquired permanently or in transit, provided

   (ii) To conduct regular cyber-security audits following appropriate national standards to maintain compliance
6. To establish clear-cut reporting channels for any form of violation of the Cyber Security and Data Privacy policies and any other specific information security and management policy as the case may be.
7. To protect TEIL stakeholders, information and assets from threats that could potentially disrupt business and TEIL brand and reputation
8. To communicate the importance of cyber security and to continually enhance information security capabilities to all the concerned

9. To ensure compliance with this policy by all concerned in the respective Business Heads/Department Heads in their respective business domains
10. To report periodically all breaches of information security, actual or suspected, and thereafter the same be investigated by the designated/assigned personnel and to take appropriate corrective and preventive actions
11. Training and Communication:

    The Company shall provide regular information security awareness to employees or any external person who may have access or use the company's information systems and data. The awareness shall cover topics such as:

    - Information security policies and procedures
    - Phishing and social engineering
    - Incident reporting and response

This policy also applies to all information, computer, and data communication systems owned, licensed, and administered by TEIL. The content and robustness of implementation of this policy will be reviewed periodically and revised accordingly, as needed.