GRAPHITE INDIA LIMITED

REGD. & H.0.: 31, CHOWRINGHEE ROAD, KOLKATA - 700 016, W.B., INDIA PHONE: 91 33 4002 9600, 2226 5755 /4942 / 4943 / 5547 / 2334, 2217 1145/ 1146 FAX: 91 33 2249 6420, E-mail: gilro@graphiteindia.com WEBSITE www.graphiteindia.com, CIN: L10101WB1974PLCO94602

Information Security & Cyber Security Policy

1. PURPOSE

Graphite India Limited (hereafter referred to as "GIL" or "the Company") recognizes that information and digital assets are critical to its business operations, regulatory compliance, operational safety, intellectual property protection, and stakeholder trust. GIL operates complex manufacturing facilities supported by engineering systems, plant automation, enterprise platforms, supply chain networks, and digital communication systems.

This Policy establishes a structured framework to safeguard the confidentiality, integrity, availability, and privacy of GIL's information assets and information processing systems, while ensuring resilience against cyber threats, operational disruptions, and data misuse.

2. SCOPE

This Policy applies to:

- All information assets owned, managed, or processed by GIL.
- All information systems including Enterprise Resource Planning (ERP), Operational Technology (OT) systems, plant automation and control systems, engineering and design systems, laboratory systems, finance & sales platforms, cloud services, and communication networks.
- All GIL employees, contract workers, consultants, suppliers, contractors, service providers, logistics partners, and other third parties who access GIL information or systems.

3. REGULATORY AND STANDARDS ALIGNMENT

GIL's Information Security framework is aligned with applicable laws, regulations, and recognized best practices, including the Information Technology Act, 2000, the Digital Personal Data Protection Act (DPDP Act), 2023, and other relevant regulatory requirements. The framework also aligns with internationally recognized standards such as ISO/IEC 27001 (Information Security Management), ISO/IEC 27701 (Privacy Information Management), the NIST Cybersecurity Framework, and other industry best practices, as applicable.

4. POLICY STATEMENT

GIL is committed to:

- Protecting business, operational, technical, financial, regulatory, and personal data from unauthorized access, loss, misuse, alteration, or disclosure.
- Integrating information security into all business processes, plant operations, engineering activities, and corporate functions.

REGD. & H.0.: 31, CHOWRINGHEE ROAD, KOLKATA - 700 016, W.B., INDIA PHONE: 91 33 4002 9600, 2226 5755 /4942 / 4943 / 5547 / 2334, 2217 1145/ 1146 FAX: 91 33 2249 6420, E-mail: gilro@graphiteindia.com WEBSITE www.graphiteindia.com, CIN: L10101WB1974PLCO94602

- Conducting periodic risk assessments to identify threats, vulnerabilities, and control gaps.
- Classifying and handling information based on sensitivity, confidentiality, and criticality.
- Implementing appropriate physical, technical and administrative security controls.
- Taking disciplinary action for violations of this Policy in accordance with applicable rules and procedures.

5. CYBERSECURITY OBJECTIVES

GIL's cybersecurity objectives include:

- **Leadership Commitment:** Strong management oversight and accountability for information security and cyber risk management.
- **Risk Management:** Identification and mitigation of cyber risks across IT and OT environments.
- **Data Protection:** Safeguarding confidentiality, integrity, and availability of information assets.
- **Incident Management:** Timely detection, reporting, investigation and resolution of cybersecurity incidents.
- **Third-Party Security:** Ensuring suppliers, contractors, and service providers meet GIL's security expectations through periodic audits and due diligence.
- **Awareness & Training:** Building a security-conscious workforce across plants, offices, and project sites.
- **Continuous Improvement:** Strengthening the security posture through audits, reviews, and evolving controls.

6. CYBERSECURITY APPROACH

a. Governance & Risk Integration

- Cyber risks are integrated into GIL's enterprise risk management framework.
- Security-by-design principles are applied during system procurement, implementation, and upgrades.

b. IT and OT Security

- Protection of plant automation systems, industrial control systems, furnace operations, and laboratory equipment.
- Segregation of Operational Technology (OT) networks from corporate IT networks.
- Regular patching, vulnerability management, and monitoring of legacy systems.

c. Data Protection & Privacy

- Secure handling of employee, customer, supplier, and stakeholder data.
- Role-based access controls and data minimization practices.

REGD. & H.0.: 31, CHOWRINGHEE ROAD, KOLKATA - 700 016, W.B., INDIA PHONE: 91 33 4002 9600, 2226 5755 /4942 / 4943 / 5547 / 2334, 2217 1145/ 1146 FAX: 91 33 2249 6420, E-mail: gilro@graphiteindia.com WEBSITE www.graphiteindia.com, CIN: L10101WB1974PLCO94602

- Compliance with applicable data protection laws including consent, retention, and disclosure requirements under the DPDP Act.

d. Network & Infrastructure Security
   - Implementation of layered security controls such as firewalls, endpoint protection, intrusion detection systems, and access controls.
   - Secure remote access mechanisms for authorized users.
   - Continuous monitoring of network traffic, system logs, and security events.

e. Cloud & Third-Party Risk
   - Secure use of cloud platforms in line with industry standards and contractual safeguards.
   - Vendor risk assessments and contractual security obligations.
   - Controlled access for suppliers, contractors, and service providers.

f. Physical Security
   - Restricted access to server rooms, control rooms, data centers, and sensitive operational areas.
   - Surveillance and access control mechanisms at critical facilities.
   - Protection of physical records, engineering drawings, and confidential documents.

g. Business Continuity & Resilience
   - Backup and recovery mechanisms for critical systems and data.
   - Disaster recovery and business continuity planning for essential operations.
   - Incident response procedures aligned with organizational crisis management plans.

7. TRAINING AND AWARENESS

GIL will:

- Conduct periodic information security awareness programs for employees and contractors.
- Provide role-based training for high-risk functions such as IT, engineering, finance, procurement, and operations.
- Promote awareness of phishing, social engineering, safe digital practices and secure handling of information assets.

8. ROLES AND RESPONSIBILITIES

- **Business and Plant Heads:** Ensure compliance with this Policy within their respective areas.
- **Employees and Contractors:** Protect information assets and adhere to security procedures and guidelines.

REGD. & H.O.: 31, CHOWRINGHEE ROAD, KOLKATA - 700 016, W.B., INDIA PHONE: 91 33 4002 9600, 2226 5755 /4942 / 4943 / 5547 / 2334, 2217 1145/ 1146 FAX: 91 33 2249 6420, E-mail: gilro@graphiteindia.com WEBSITE www.graphiteindia.com, CIN: L10101WB1974PLCO94602

- **Information Technology Team:** Implement security controls, monitor risks, manage incidents, and report to management.
- **Third Parties:** Comply with GIL's information security requirements as part of contractual obligations.

9. INCIDENT REPORTING, COMPLIANCE AND DISCIPLINARY ACTION

All suspected or actual information security incidents or breaches involving GIL's information assets must be reported promptly through designated internal channels or complaints may also be reported through the mechanisms defined under the Company's Whistleblower Policy or Grievance Redressal Policy, as applicable. GIL's IT Team will investigate reported incidents in a timely manner and implement appropriate corrective and preventive actions. Non-compliance with this Policy, failure to report incidents, or any deliberate violation may result in disciplinary action for employees, termination or suspension of contracts for third parties, and legal or regulatory action wherever applicable.

10. GOVERNANCE

- The policy is approved by the Executive Director of GIL. The Head of IT shall oversee the implementation of this Policy, and the Information Technology function shall be responsible for its operational execution.
- This Policy shall be reviewed periodically, or earlier if required, due to changes in business operations, technology, threat landscape, or regulatory requirements.
- The Policy will be communicated to employees, contractors, and relevant stakeholders through appropriate platforms.

DATE: 18.12.2025

A. DIXIT

EXECUTIVE DIRECTOR