



SARDA ENERGY & MINERALS LIMITED

Regd. Off: 73-A, Central Avenue, Nagpur (MH.) 440018
Ph: +91-712-2722407; Fax: +91-712-2722107 Email: cs@seml.co.in
URL: www.seml.co.in CIN: L27100MH1973PLC016617

Information and Cyber Security Policy

1. Preamble

Sarda Energy & Minerals Limited ("SEML" or "the Company") recognises that information and technology assets are critical to the integrity, efficiency and sustainability of its business operations. In an increasingly digital and interconnected environment, threats to information security and cyber resilience can result in operational disruption, financial loss, regulatory exposure and reputational damage.

SEML is therefore committed to establishing a structured and proactive approach to protect its information assets and technology systems against unauthorised access, misuse, disruption, destruction and cyber-attacks.

2 Objectives of the Policy

The objective of this Policy is to define a framework for managing information and cyber security risks across SEML and to ensure confidentiality, integrity and availability of information assets. This Policy aims to:

- i) Safeguard business, operational, personal and confidential information;
- ii) Protect IT and operational technology ("OT") systems from cyber threats;
- iii) Ensure compliance with applicable laws and regulatory requirements;
- iv) Promote cyber-safe behaviour among employees and associates; and
- v) Enable secure and resilient business operations.

3 Effective Date

This Policy comes into effect from 23.05.2026.

4. Scope and Applicability

This Policy applies to:

- i) All information assets, whether electronic, physical or otherwise;
- ii) All information technology and operational technology systems;
- iii) All SEML locations, plants, offices and project sites; and
- iv) All employees, directors, contractors, consultants, vendors and third parties who access SEML's information or systems.

5 Governance and Accountability

The Board of Directors shall have overall oversight of information and cyber security governance.

- i) Senior Management shall be responsible for implementing this Policy and ensuring adequate controls and resources.
- ii) The Information Technology / Cyber Security function shall be responsible for day-to-day management, monitoring and response.
- iii) Line managers shall ensure compliance within their functions.
- iv) All users of SEML's information assets shall be accountable for adherence to this Policy.



SARDA ENERGY & MINERALS LIMITED

Regd. Off: 73-A, Central Avenue, Nagpur (MH.) 440018
Ph: +91-712-2722407; Fax: +91-712-2722107 Email: cs@seml.co.in
URL: www.seml.co.in CIN: L27100MH1973PLC016617

6 Information Security Principles

SEML's information and cyber security practices are guided by the following core principles:

- i) Information shall be protected throughout its lifecycle;
- ii) Access to information shall be based on business need and authorisation;
- iii) Risks shall be identified and mitigated proactively;
- iv) Security requirements shall be embedded into business processes and systems; and
- v) Security controls shall be reviewed and improved continuously.

7 Protection of Information Assets

SEML shall protect all information assets to ensure their confidentiality, integrity and availability. This includes:

- i) Maintaining an inventory of key information and technology assets;
- ii) Classifying information based on sensitivity and criticality;
- iii) Protecting intellectual property, business data and confidential information; and
- iv) Preventing unauthorised access, disclosure, alteration or loss.

8 Identity and Access Management

Access to SEML's information and systems shall be controlled through appropriate identity and access management practices.

- i) Users shall be granted access only to the extent necessary to perform their roles.
- ii) Access rights shall be reviewed periodically.
- iii) Authentication and authorization mechanisms shall be implemented to prevent misuse.

9 Acceptable Use of Information and Technology Assets

All users shall use SEML's information and technology resources responsibly and for legitimate business purposes. Unauthorised use, sharing of passwords, download of malicious software or misuse of systems is strictly prohibited.

10 Cyber Risk Management

Cyber security risks shall be identified, assessed and managed as part of SEML's overall risk management framework.

- i) Security risks arising from IT systems, OT systems, projects and third-party engagements shall be evaluated.
- ii) Appropriate preventive, detective and corrective controls shall be implemented.
- iii) Cyber security considerations shall be incorporated at the design stage of new systems and projects.

11 Third-Party and Supply Chain Security

SEML expects third-party service providers and vendors handling its information or systems to adhere to appropriate information security practices.

- i) Cyber security requirements shall be incorporated into relevant contracts and agreements.
- ii) Third-party access shall be monitored and controlled.
- iii) Material security incidents involving third parties shall be reported and addressed promptly.



SARDA ENERGY & MINERALS LIMITED

Regd. Off: 73-A, Central Avenue, Nagpur (MH.) 440018
Ph: +91-712-2722407; Fax: +91-712-2722107 Email: cs@seml.co.in
URL: www.seml.co.in CIN: L27100MH1973PLC016617

12 Data Protection and Privacy

Personal and sensitive data handled by SEML shall be protected in accordance with applicable data protection and privacy laws.

- i) Collection and processing of personal data shall be lawful and purpose-bound.
- ii) Reasonable safeguards shall be implemented to prevent data breaches.
- iii) Data retention and disposal shall follow defined retention principles.

13 Cyber Security Incident Management

SEML shall maintain mechanisms to detect, respond to and recover from cyber security incidents.

- i) All suspected or actual cyber incidents shall be reported promptly.
- ii) Incidents shall be investigated to identify root causes.
- iii) Corrective actions shall be implemented to prevent recurrence.
- iv) Learnings shall be communicated where relevant.

14 Business Continuity and Backup

Information and cyber security controls shall support SEML's business continuity and disaster recovery arrangements.

- i) Critical systems and data shall be backed up appropriately.
- ii) Recovery procedures shall be tested periodically.
- iii) Cyber resilience shall form part of business continuity planning.

15 Training and Awareness

SEML shall promote information security awareness across the organisation.

- i) Employees shall be provided appropriate training on cyber risks and safe practices.
- ii) Awareness programmes shall be conducted periodically to address emerging threats.
- iii) Compliance with security practices shall be reinforced through communication and leadership.

16 Monitoring, Audit and Compliance

SEML shall periodically monitor and assess the effectiveness of information and cyber security controls.

- i) Internal reviews and audits may be conducted.
- ii) Identified gaps shall be addressed in a timely manner.
- iii) Non-compliance may result in disciplinary or contractual action, as applicable.

17 Review

This Policy shall be reviewed periodically and updated as necessary to address changes in technology, business operations, regulatory requirements and risk landscape.