MOIL LIMITED

Information Technology (IT) Policy-2017

1. Introduction

MOIL Limited (MOIL) is a Schedule-A Central Public Sector Enterprise (CPSE) under administrative control of Ministry of Steel, Government of India. It is the largest mining company in India and produces about 50% of total production of manganese ore in the country.

MOIL is committed to create appropriate Information Technology (IT) infrastructure to support its business function and organisational growth in most secured manner, and to use IT as the vital tool in improving efficiency, productivity, decision-making, transparency and cost effectiveness, and thus adding value to the business particularly in the ERP environment.

This policy has been framed to provide a broad framework about IT and its usage.

2. Effective Date

This policy shall be known as MOIL Information Technology Policy-2017 (the "Policy") and shall become effective from the date of its approval by the Board.

3. Objective

The objective of this policy is to:

- ensure electronic delivery of services to all stakeholders and business across all departments and functions to achieve the objective of transparency and efficiency
- maintain confidentiality of data and to protect IT assets against unauthorised disclosure
- ensure integrity of data, and availability and accessibility of IT systems as and when required.

4. Scope of the Policy

This policy applies to all MOIL IT systems and those working at or for MOIL (Users): (1) All MOIL employees (2) Contractors, agencies, vendors, customers and other outside agencies, where they are directly using MOIL's network. (3) Employees on deputation to MOIL from other organisations.

5. Definitions of Key IT terms used

- **Security breach**: A security breach is any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms.
- **Security incident** : A security incident is an event that may indicate that an organization's systems or data have been compromised or that measures put in place to protect them have failed
- **Disaster Recovery**: Disaster recovery involves a set of procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.
- **Firewall**: A firewall is a network security system, either hardware- or software-based, that uses rules to control incoming and outgoing network traffic.

6. Responsibility

(i) The Head of Systems Department will be responsible for implementation of the policy. He is *inter-alia* responsible for monitoring and reporting on the state of IT systems and security.

(ii) Internal Procedural parts will be framed in line with this policy with the approval of CMD for execution and administration.

7. Unacceptable Use of IT

- Violations of the rights of any person protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of pirated or other software products that are not appropriately licensed for use by MOIL.
- Not to engage in any activity that is illegal under local, state, national and international law while utilizing MOIL's IT assets.
- Use of unauthorized software.

8. Security and Security incident investigation and reporting

The objective of security incident investigation is to identify, detect, investigate and resolve any suspected or actual computer security breach. All security or any concerns or suspicions about security breaches should be reported, as soon as they arise.

IT systems are always subject to high degree of risks and therefore continue to be given top priority, and for this purpose:

- Licensed anti-virus should be installed and should be updated on regular basis.
- Firewall should be installed to protect the MOIL network from external attack.
- Back-up of critical data and system configurations on a regular basis and storage of data in a safe place.
- All security threats/incidents will be formally recorded and categorised by severity and actions taken thereon should also be recorded in accordance with prescribed procedure. Provision for safeguarding / protection of confidentiality of data / information be put in place especially with regard to sensitive information including Aadhar, etc. in line with Government guidelines.
- Users of IT system be imparted training on usage of related guidelines and procedures.

9. Access controls

(I) Physical access

- An entry restriction system to the server/Data Center at all premises should be implemented.
- No remote access to IT systems should be given to third parties at any time unless specific authorisation is received. Such access, if granted, must be supervised at all times.
- Inter unit or Inter department movement of IT assets should be done with proper authorization.

(II) Application access

- Each application can be accessed by authorized employees/persons only.
- Users should be activated by system administrator wherever necessary.
- Role of Application Developer should be segregated from System Administrator role for better control wherever possible.

10. Disaster recovery and business continuity

- Proper backup schedules should be maintained to ensure availability of missing data at any point of time.
- A robust disaster recovery plans should be in place to minimise the risk to MOIL's IT systems from different incidents.
- Emergency procedures covering immediate actions to be taken in response to an incident (e.g. alerting disaster recovery personnel/team) should also be in place.

11. Maintenance of official website of the Company

- Contents uploaded on the website be regularly updated and archived as per relevant archival policy.
- All content on the website should have proper approval or authorisation before it is published and should be reviewed on regular basis.
- Guidelines issued by Government/Government agencies regarding security, contents, design, style, etc. of the website from time to time should be followed.
- All information published on the website should meet prescribed statutory requirements to bring more transparency about the working of the company.

12. Email Communication and usage of Internet & Social Media

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam) should be avoided. Any form of harassment via email, whether through language, frequency, or size of messages would be considered offence and subject to disciplinary action.
- Official communications through e-mail to be done using official e-mail ID unless there is any operational issue.
- Use of social media (like Twitter. Facebook, etc.) should be done wherever possible to communicate with the stakeholders to inform them about various developments and activities of the company. However, contents published on the social media should have proper authorisation and to be handled only by designated persons for this purpose.
- No objectionable, frivolous or illegal activity should be carried out on internet that shall damage the company's business or its image.

13. Auditors and Compliance

- The implementation of MOIL's IT policy and procedures will be subject to periodic review by internal and also by external auditors wherever necessary.
- Breach of this policy would invite disciplinary action, wherever necessary.
- Periodical compliance report in respect of IT related laws will be submitted to the Board of Directors.

14. Amendment/Modifications

Any amendment/modification to this policy shall require approval of the Board of Directors of MOIL.

*****