OVERALL GUIDING PRINCIPLE OF INFORMATION SECURITY

HPCL-Mittal Energy Limited & its' Subsidiary

Version	Modification Date	Section	Amendment / Modification / Deletion	Brief Description of Change
1.0	September 2023			Launch

1. Our guiding principle statements

These guidelines are overall declaration by HPCL-Mittal Energy Limited (HMEL) of the Information security objectives and expectations, which allows utilization of information systems for effective and efficient achievement of business goals. We are committed to establish and consistently improve cybersecurity posture, processes and minimize exposure to potential risks.

2. Scope and applicability

These guidelines apply to HMEL employees, customers and partners who have access to HMEL information or are involved in management of information systems. These guidelines shall also be applicable for all subsidiaries of HMEL.

3. Definitions

i) **Information**: Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative or audio visual

ii) **Information Security**: Protecting information and information system from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability

iii) **Information Security Event**: An identified occurrence of a system, service or network state indicating a possible breach of information.

iv) **Incident**: An occurrence that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits or that constitutes a violation or imminent threat of violation of security and it's procedures.

v) **Information Security Incident**: a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

vi) **Risk**: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of the likelihood of occurrence and the adverse impacts which would arise if the circumstance or event occurs

vii) **Confidentiality**: Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information

viii)**Integrity**: Safeguarding the accuracy and completeness of assets against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity

ix) **Availability**: Ensuring timely and reliable access to and use of information

x) **Risk Management:** Coordinated activities to direct and control an organization regarding risk

xi) **Risk Analysis:** Systematic use of information to identify sources and to estimate the risk

4. Information Security Principles

HMEL Guiding principles of information technology is a framework to ensure that its information is comprehensively protected against the consequences of breaches of confidentiality, failures of integrity, interruptions to their availability, loss of authenticity and/or repudiation of an action. HMEL intends to achieve this by :

a) Ensuring compliance with all applicable **standards, regulatory and legal requirements.**

b) Applying effective **risk management framework** to identify, manage and mitigate risks associated with HMEL through undertaking a vulnerability assessment.

c) Protect all HMEL **information assets** from possible threats which could potentially disrupt the business and functioning of HMEL.

d) A **backup management system** for creating copies of information which is essential to recover and restore original data in the event of data loss.

e) Consistently **improve and upgrade technology**, systems, and processes to protect HMEL against known and unknown cybersecurity threats.

f) Implement **incident management** procedures for detecting, reporting, and responding to incidents.

g) Provision access to information systems based on **least privileged access model** and **segregation of duties.**

h) Applying **business continuity and disaster recovery management** controls to increase the preparedness of the organization against any crisis/ disaster.

i) Applying **Third Party Security** controls to manage the contracts, services and changes provided by vendors/ partners.

j) Applying effective **Physical and Environment Security** controls to protect the information system from physical and environmental threats.

k) Implementing strong controls for **protection against malicious software** to protect the HMEL environment against malware.

l) A **change management system** to ensure changes in the IT environment are implemented in a controlled manner.

m) Effective **capacity management controls** to ensure that use of IT resources is monitored, tuned and future capacity requirements are projected.

n) HMEL recognizes the critical importance of data privacy in our operations. We are committed to protecting the confidentiality, integrity and availability of all personal data entrusted to us by our customers, employees, and partners.

5. Compliance to these guidelines

All employees are encouraged to report any suspicious activity to the Information Security team through designated channels. All reported incidents shall be handled in a proper and timely manner with corrective actions being implemented immediately without comprising on the confidentiality, integrity, and availability of information of HMEL.

The information security team regularly conducts violation checks across the HMEL ecosystem and adequate provisions have been designed and implemented to handle any non- compliances. In addition to regular process adherence checks (PACs), vulnerability assistance(VA) and penetration test (PA) are regularly conducted to continually check security posture of the organization.

6. Roles and Responsibilities of Information Security team

HMEL Information Security team is responsible for establishing and maintaining an Information Security Management System (ISMS) aligned with ISO 27001, ensuring the confidentiality, integrity, and availability of our information assets. In addition, the team is also responsible for the below.

- **Risk Management and Compliance**: The team assesses risks, develops mitigation strategies, and monitors compliance with ISO 27001 and NIST 800-82 standards, ensuring that information security measures evolve to address emerging threats and vulnerabilities.

- **Business Continuity and Disaster Recovery:** In accordance with ISO 22301, HMEL Information Security team plans, tests, and maintains business continuity and disaster recovery strategies, ensuring the resilience of critical business processes and IT systems in the face of disruptions.

- **Incident Response and Security Awareness**: HMEL Information Security team is also responsible for swift incident response, investigation, and communication in the event of security incidents, while also promoting a culture of security awareness and training among all employees.

- **Continuous Improvement:** Team is committed to ongoing improvement by conducting regular security audits, reviews, and updates to these guidelines and controls to stay ahead of evolving security threats and regulatory requirements.

7. Governance

HMEL Apex committee (chaired by MD&CEO) and Head-IT are responsible for overseeing cybersecurity governance as per HMEL's Risk Management Framework. Reports pertaining to cybersecurity risks are to be presented from the Information Security team to the Apex committee part of regular reviews with Top management.

Information Security lead is responsible for clearly outlining expectations, providing support in implementing and monitoring progress on safeguarding HMEL information and assets. The Information Security strategy, policy, and cybersecurity programs are to be driven with a top-down approach from the Information Security lead to all business units and function heads further down to all the employees. Business units and function heads are responsible for implementing adequate security policies, process, and controls to protect confidentiality, maintain integrity and ensure availability of all information assets.

8. Exception Management

All exceptions regarding these guidelines will be directed to the Information Security team. The exception request will be formally recorded in writing and reviewed by the Information Security Team before formally arriving at a decision to approve or reject the exception request. The validity of the exception shall be defined and not exceed one year. An annual review of all accepted exceptions shall be carried out by the Information Security team to identify any changes in risk posed by the exception or to identify alternate controls that could be implemented to reduce the risk.

9. Trainings and awareness

All HMEL employees are required to attend awareness programs on Information Security with regular trainings made available by the management. HMEL will educate employees upon hiring and conduct awareness program through emails, posters, talks in employees gatherings, meetings and annual cybersecurity festival.

10. Review

These guidelines will be reviewed on an annual basis or in case of any significant changes to check for effectiveness, changes in technology and changes in risk levels that may have an impact on confidentiality, integrity and availability, legal and contractual requirements, and business efficiency.

11. **References Standards**

HMEL's Information guiding principles is aligned with the following global security standards:

- ISO/IEC 27001:2013
- ISO/IEC 22301: 2019
- NIST 800-82
- CERT-IN

HMEL is certified with ISO/IEC 27001:2013, ISO/IEC 22301:2019 and ISO/IEC 20000-1:2018 with a year-on-year external audit from industry recognized tier-1 certification bodies.

Harak Banthia
CFO

Prabh Das
MD & CEO

September 30, 2023

HMEL®